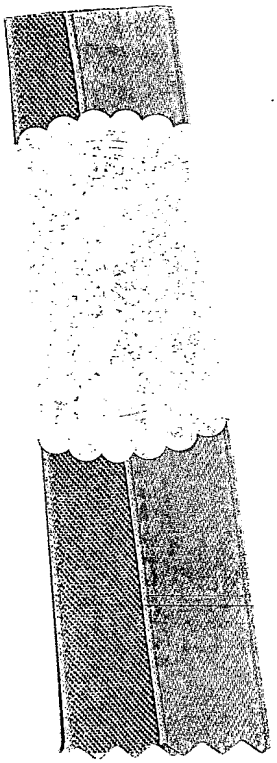
日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　１月２６日

出願番号
Application Number: 特願２０００－０１６５４５

出願人
Applicant (s): ソニー株式会社
株式会社ソニー・コンピュータエンタテインメント



PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(A) OR (B)

２０００年１２月　８日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３１０２４６７

【書類名】　特許願

【整理番号】　99008900

【提出日】　平成12年 1月26日

【あて先】　特許庁長官殿

【国際特許分類】　G09C　1/00

【発明の名称】　データ処理システム、記録デバイス、およびデータ処理方法、並びにプログラム提供媒体

【請求項の数】　25

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　石橋　義人

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　浅野　智之

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　秋下　徹

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　白井　太三

【発明者】

【住所又は居所】　東京都港区赤坂７丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内

【氏名】　吉森　正治

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【特許出願人】

【識別番号】　395015319

【氏名又は名称】　株式会社ソニー・コンピュータエンタテインメント

【代表者】　久夛良木　健

【代理人】

【識別番号】　100101801

【弁理士】

【氏名又は名称】　山田　英治

【電話番号】　03-5541-7577

【選任した代理人】

【識別番号】　100093241

【弁理士】

【氏名又は名称】　宮田　正昭

【電話番号】　03-5541-7577

【選任した代理人】

【識別番号】　100086531

【弁理士】

【氏名又は名称】　澤田　俊夫

【電話番号】　03-5541-7577

【手数料の表示】

【予納台帳番号】　062721

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　　要約書　1

【物件名】　　委任状　1

【提出物件の特記事項】　委任状は後日提出

【包括委任状番号】　9904833

【プルーフの要否】　　要

【書類名】　　明細書

【発明の名称】　データ処理システム、記録デバイス、およびデータ処理方法、並びにプログラム提供媒体

【特許請求の範囲】

【請求項１】

相互に暗号データの転送を実行する第1の装置と第２の装置とからなるデータ処理システムにおいて、

前記第2の装置は、前記第1の装置との転送データに関する暗号処理を実行する暗号処理部を有し、

該暗号処理部は、

前記第1の装置から転送されるコマンド識別子を予め定められた設定シーケンスにしたがって受領し、該受領コマンド識別子に対応するコマンドをレジスタから取り出して実行させる制御部を有し、

該制御部は、前記第1の装置から転送されるコマンド識別子が前記設定シーケンスと異なるコマンド識別子である場合には、該コマンド識別子に対応するコマンドの処理を中止する構成を有することを特徴とするデータ処理システム。

【請求項２】

前記制御部の有する前記第1の装置から受領するコマンド識別子に関する設定シーケンスは、順次、番号がインクリメントされるコマンド番号設定シーケンスであり、

前記制御部は、前記第1の装置からの受領コマンド番号の受付値をメモリに格納するとともに、前記第1の装置からの新規受領コマンド番号を、前記メモリに格納さた受付済みコマンド番号に基づいて設定シーケンスとの一致を判定し、設定シーケンスと異なると判定された場合には、該新規受領コマンド番号に対応するコマンド処理を行なわず、前記メモリに格納したコマンド番号のリセットを実行する構成を有することを特徴とする請求項１に記載のデータ処理システム。

【請求項３】

前記第2の装置は、前記設定シーケンスに従ったコマンドを格納したコマンドレジスタを有し、

前記コマンドレジスタには、

前記第1の装置と前記第2の装置との認証処理を実行する認証処理コマンドシーケンスと、

前記第1の装置と前記第2の装置との間における転送データに関する暗号処理を実行する暗号処理コマンドシーケンスとが格納されており、

前記認証処理コマンドシーケンスに対応するコマンド識別子は、前記暗号処理コマンドシーケンスに対応するコマンド識別子より以前のステップにおいて実行されるようにシーケンス設定がなされていることを特徴とする請求項１に記載のデータ処理システム。

【請求項４】

前記暗号処理コマンドシーケンスは、

前記第1の装置から前記第2の装置に対して転送され、前記第2の装置内の記憶手段に格納される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、または、

前記第2の装置内の記憶手段に格納され、前記第２の装置から前記第１の装置に対して転送される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、

少なくとも上記いずれかのコマンドシーケンスを含むことを特徴とする請求項３に記載のデータ処理システム。

【請求項５】

前記制御部は、

前記第1の装置と前記第2の装置との認証処理により認証が成立した場合に、認証済みであることを示す認証フラグを設定し、該認証フラグが設定されている間は、前記暗号処理コマンドシーケンスの実行を可能とするコマンド管理制御を実行し、

前記制御部は、

前記認証処理コマンドシーケンスを新たに実行する際に前記認証フラグをリセットすることを特徴とする請求項３に記載のデータ処理システム。

【請求項６】

前記制御部は、

前記暗号鍵交換処理において、前記設定シーケンスおよびコマンド識別子に基づいてコマンド実行順序を管理し、

前記制御部は、前記鍵交換処理に関する一連のコマンド実行中は、前記第1の装置を含む外部装置からの前記設定シーケンスと異なるコマンド処理を受け付けない構成であることを特徴とする請求項４に記載のデータ処理システム。

【請求項７】

前記第2の装置は、暗号化データを記憶するデータ記憶部を有する記憶デバイスであり、

前記第1の装置は、前記記憶デバイスに対するデータの格納処理、および前記記憶デバイスに格納されたデータを取り出して再生、実行を行なう記録再生器であり、

前記記録再生器は、前記記録デバイスとの転送データの暗号処理を実行する暗号処理部を有することを特徴とする請求項１に記載のデータ処理システム。

【請求項８】

前記記録デバイスは、

前記記録再生器と記録デバイス間の認証処理に適用する認証鍵、および前記記録デバイス内のデータ記憶部に格納するデータの暗号化鍵としての保存鍵を格納した鍵ブロックを有し、

前記記録デバイスの暗号処理部における前記制御部は、

前記記録再生器から前記設定シーケンスにしたがってコマンド識別子を受領して前記鍵ブロックに格納した認証鍵を用いた認証処理を実行し、該認証処理完了後に前記保存鍵を用いた鍵交換処理を伴うデータの暗号処理を実行する構成であることを特徴とする請求項７に記載のデータ処理システム。

【請求項９】

前記鍵ブロックは、それぞれ異なる認証鍵および保存鍵を格納した複数の鍵ブロックから構成され、

前記記録再生器は、前記複数の鍵ブロックから、認証処理およびデータの暗号処理に使用する１つの鍵ブロックを指定鍵ブロックとして前記記録デバイスに通

知し、前記記録デバイスは、指定鍵ブロックに格納された認証鍵を用いた認証処理、および保存鍵を用いたデータの暗号処理を実行する構成であることを特徴とする請求項８に記載のデータ処理システム。

【請求項１０】

外部装置との間で転送可能なコンテンツデータを記憶するデータ記憶部を有する記録デバイスであり、

前記記録デバイスは、外部装置との転送データに関する暗号処理を実行する暗号処理部を有し、

該暗号処理部は、

外部装置から転送されるコマンド識別子を予め定められた設定シーケンスにしたがって受領し、該受領コマンド識別子に対応するコマンドをレジスタから取り出して実行させる制御部を有し、

該制御部は、前記外部装置から転送されるコマンド識別子が前記設定シーケンスと異なるコマンド識別子である場合には、該コマンド識別子に対応するコマンドの処理を中止する構成を有することを特徴とする記録デバイス。

【請求項１１】

前記制御部は、前記設定シーケンスとして、順次、番号がインクリメントされるコマンド番号設定シーケンスを有し、

前記制御部は、前記外部装置からの受領コマンド番号の受付値をメモリに格納するとともに、前記外部装置からの新規受領コマンド番号を、前記メモリに格納さた受付済みコマンド番号に基づいて設定シーケンスとの一致を判定し、設定シーケンスと異なると判定された場合には、該新規受領コマンド番号に対応するコマンド処理を行なわず、前記メモリに格納したコマンド番号のリセットを実行する構成を有することを特徴とする請求項１０に記載の記録デバイス。

【請求項１２】

前記記録デバイスは、前記設定シーケンスに従ったコマンドを格納したコマンドレジスタを有し、

前記コマンドレジスタには、

前記外部装置と前記記録デバイスとの認証処理を実行する認証処理コマンドシ

ーケンスと、

前記外部装置と前記記録デバイスとの間における転送データに関する暗号処理を実行する暗号処理コマンドシーケンスとが格納されており、

前記認証処理コマンドシーケンスに対応するコマンド識別子は、前記暗号処理コマンドシーケンスに対応するコマンド識別子より以前のステップにおいて実行されるようにシーケンス設定がなされていることを特徴とする請求項１０に記載の記録デバイス。

【請求項１３】

前記暗号処理コマンドシーケンスは、

前記外部装置から前記記録デバイスに対して転送され、前記記録デバイス内の記憶手段に格納される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、または、

前記記録デバイス内の記憶手段に格納され、前記記録デバイスから前記外部装置に対して転送される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、

少なくとも上記いずれかのコマンドシーケンスを含むことを特徴とする請求項１２に記載の記録デバイス。

【請求項１４】

前記制御部は、

前記外部装置と前記記録デバイスとの認証処理により認証が成立した場合に、認証済みであることを示す認証フラグを設定し、該認証フラグが設定されている間は、前記暗号処理コマンドシーケンスの実行を可能とするコマンド管理制御を実行し、

前記制御部は、

前記認証処理コマンドシーケンスを新たに実行する際に前記認証フラグをリセットすることを特徴とする請求項１２に記載の記録デバイス。

【請求項１５】

前記制御部は、

前記暗号鍵交換処理において、前記設定シーケンスおよびコマンド識別子に基

づいてコマンド実行順序を管理し、

前記制御部は、前記鍵交換処理に関する一連のコマンド実行中は、前記外部装置を含む外部装置からの前記設定シーケンスと異なるコマンド処理を受け付けない構成であることを特徴とする請求項１３に記載の記録デバイス。

【請求項１６】

前記記録デバイスは、

前記外部装置と記録デバイス間の認証処理に適用する認証鍵、および前記記録デバイス内のデータ記憶部に格納するデータの暗号化鍵としての保存鍵を格納した鍵ブロックを有し、

前記記録デバイスの暗号処理部における前記制御部は、

前記外部装置から前記設定シーケンスにしたがってコマンド識別子を受領して前記鍵ブロックに格納した認証鍵を用いた認証処理を実行し、該認証処理完了後に前記保存鍵を用いた鍵交換処理を伴うデータの暗号処理を実行する構成であることを特徴とする請求項１０に記載の記録デバイス。

【請求項１７】

前記鍵ブロックは、それぞれ異なる認証鍵および保存鍵を格納した複数の鍵ブロックから構成され、

前記外部装置は、前記複数の鍵ブロックから、認証処理およびデータの暗号処理に使用する１つの鍵ブロックを指定鍵ブロックとして前記記録デバイスに通知し、前記記録デバイスは、指定鍵ブロックに格納された認証鍵を用いた認証処理、および保存鍵を用いたデータの暗号処理を実行する構成であることを特徴とする請求項１６に記載の記録デバイス。

【請求項１８】

相互に暗号データの転送を実行する第1の装置と第２の装置とからなるデータ処理システムにおけるデータ処理方法であり、

前記第2の装置は、

前記第1の装置から転送されるコマンド識別子を予め定められた設定シーケンスにしたがって受領し、該受領コマンド識別子に対応するコマンドをレジスタから取り出して実行させるコマンド処理制御ステップを実行し、

前記コマンド処理制御において、前記第1の装置から転送されるコマンド識別子が前記設定シーケンスと異なるコマンド識別子である場合には、該コマンド識別子に対応するコマンドの処理を中止することを特徴とするデータ処理方法。

【請求項１９】

前記コマンド処理制御ステップにおいて、前記第1の装置から受領するコマンド識別子に関する設定シーケンスは、順次、番号がインクリメントされるコマンド番号設定シーケンスであり、

前記コマンド処理制御ステップは、

前記第1の装置からの受領コマンド番号の受付値をメモリに格納するステップと、

前記第1の装置からの新規受領コマンド番号を、前記メモリに格納さた受付済みコマンド番号に基づいて設定シーケンスとの一致を判定する判定ステップと、

前記判定ステップにおいて、設定シーケンスと異なると判定された場合には、該新規受領コマンド番号に対応するコマンド処理を行なわず、前記メモリに格納したコマンド番号のリセットを実行することを特徴とする請求項１８に記載のデータ処理方法。

【請求項２０】

前記データ処理方法において、

前記コマンド処理制御ステップは、

前記第1の装置と前記第2の装置との認証処理を実行する認証処理コマンドシーケンスと、

前記第1の装置と前記第2の装置との間における転送データに関する暗号処理を実行する暗号処理コマンドシーケンスとを、

実行するステップであり、

前記設定シーケンスは、前記認証処理コマンドシーケンスを前記暗号処理コマンドシーケンスに先行して実行するシーケンスであることを特徴とする請求項１８に記載のデータ処理方法。

【請求項２１】

前記データ処理方法において、

前記暗号処理コマンドシーケンスは、

前記第1の装置から前記第2の装置に対して転送され、前記第2の装置内の記憶手段に格納される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、または、

前記第2の装置内の記憶手段に格納され、前記第２の装置から前記第１の装置に対して転送される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、

少なくとも上記いずれかのコマンドシーケンスを含むことを特徴とする請求項２０に記載のデータ処理方法。

【請求項２２】

前記データ処理方法において、

前記第1の装置と前記第2の装置との認証処理により認証が成立した場合に認証済みであることを示す認証フラグを設定する認証フラグ設定ステップを含み、

前記コマンド処理制御ステップは、

前記認証フラグが設定されている間は、前記暗号処理コマンドシーケンスの実行を可能とするコマンド管理制御を実行することを特徴とする請求項２０に記載のデータ処理方法。

【請求項２３】

前記データ処理方法において、

前記認証処理コマンドシーケンスを新たに実行する際に前記認証フラグをリセットすることを特徴とする請求項２２に記載のデータ処理方法。

【請求項２４】

前記データ処理方法における前記コマンド処理制御ステップにおいて、

前記鍵交換処理に関する一連のコマンド実行中は、前記設定シーケンスおよびコマンド識別子に基づいてコマンド実行順序を管理し、

前記第1の装置を含む外部装置からの前記設定シーケンスと異なるコマンド処理を受け付けないことを特徴とする請求項２１に記載のデータ処理方法。

【請求項２５】

相互に暗号データの転送を実行する第1の装置と第２の装置とからなるデータ

処理システムにおけるデータ処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、

前記第1の装置から前記第2の装置に転送されるコマンド識別子を予め定められた設定シーケンスにしたがって受領し、該受領コマンド識別子に対応するコマンドをレジスタから取り出して実行させるコマンド処理制御ステップを有し、

前記コマンド処理制御ステップにおいて、前記第1の装置から転送されるコマンド識別子が前記設定シーケンスと異なるコマンド識別子である場合には、該コマンド識別子に対応するコマンドの処理を中止するステップを含むことを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、データ処理システム、記録デバイス、およびデータ処理方法、並びにプログラム提供媒体に関し、さらに詳細には、データ転送を実行する２つの装置間において相互認証処理を必須要件として実行させ、認証処理の成立を条件としてコンテンツの利用を可能ならしめる構成を実現するデータ処理システム、記録デバイス、データ処理方法に関する。

【０００２】

本発明は、ＤＶＤ、ＣＤ等の記憶媒体、あるいはＣＡＴＶ、インターネット、衛星通信等の有線、無線各通信手段等の経路で入手可能な音声、画像、ゲーム、プログラム等の各種コンテンツを、ユーザの所有する記録再生器において再生し、専用の記録デバイス、例えばメモリカード、ハードディスク、ＣＤ－Ｒ等に格納するとともに、記録デバイスに格納されたコンテンツを利用する際、コンテンツ配信側の希望する利用制限を付す構成を実現するとともに、この配布されたコンテンツを、正規ユーザ以外の第三者に不正利用されないようにセキュリティを確保する構成および方法に関する。

【０００３】

【従来の技術】

昨今、ゲームプログラム、音声データ、画像データ、文書作成プログラム等、

様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）が、インターネット等のネットワークを介して、あるいはＤＶＤ、ＣＤ等の流通可能な記憶媒体を介して流通している。これらの流通コンテンツは、ユーザの所有するＰＣ（Personal Computer）、ゲーム機器等の記録再生機器に付属する記録デバイス、例えばメモリカード、ハードディスク等に格納することが可能であり、一旦格納された後は、格納媒体からの再生により利用可能となる。

【０００４】

従来のビデオゲーム機器、ＰＣ等の情報機器において使用されるメモリカード装置の主な構成要素は、動作制御のための制御手段と、制御手段に接続され情報機器本体に設けられたスロットに接続するためのコネクタと、制御手段に接続されデータを記憶するための不揮発性メモリ等である。メモリカードに備えられた不揮発性メモリはＥＥＰＲＯＭ、フラッシュメモリ等によって構成される。

【０００５】

このようなメモリカードに記憶されたデータ、あるいはプログラム等の様々なコンテンツは、再生機器として利用されるゲーム機器、ＰＣ等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により不揮発性メモリから呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。

【０００６】

ゲームプログラム、音楽データ、画像データ等、多くのソフトウエア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウエアの使用を許諾し、許可のない複製等が行われないようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

【０００７】

ユーザに対する利用制限を実現する１つの手法が、配布コンテンツの暗号化処理である。すなわち、例えばインターネット等を介して暗号化された音声データ、画像データ、ゲームプログラム等の各種コンテンツを配布するとともに、正規

ユーザであると確認された者に対してのみ、配布された暗号化コンテンツを復号する手段、すなわち復号鍵を付与する構成である。

【０００８】

暗号化データは、所定の手続きによる復号化処理によって利用可能な復号データ（平文）に戻すことができる。このような情報の暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

【０００９】

暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類あるが、その１つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にＤＥＳ（データ暗号標準：Deta encryption standard）がある。

【００１０】

上述の暗号化処理、復号化に用いられる暗号化鍵、復号化鍵は、例えばあるパスワード等に基づいてハッシュ関数等の一方向性関数を適用して得ることができる。一方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザが決めたパスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵、復号化鍵を生成するものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるパスワードを求めることは実質上不可能となる。

【００１１】

また、暗号化するときに使用する暗号化鍵による処理と、復号するときに使用する復号化鍵の処理とを異なるアルゴリズムとした方式がいわゆる公開鍵暗号化方式と呼ばれる方式である。公開鍵暗号化方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が発行した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書

は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号処理が可能となる。秘密鍵は、公開鍵を発行した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号化方式の代表的なものにはＲＳＡ（Rivest-Shamir-Adleman）暗号がある。

【００１２】

このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザに対してのみ復号可能とするシステムが可能となる。これらの暗号方式を採用した従来のコンテンツ配布構成について図１を用いて簡単に説明する。

【００１３】

図１は、ＰＣ（パーソナルコンピュータ）、ゲーム機器等の再生手段１０において、ＤＶＤ，ＣＤ３０、インターネット４０等のデータ提供手段から取得したプログラム、音声データ、映像データ等（コンテンツ（Content））を再生するとともに、ＤＶＤ，ＣＤ３０、インターネット４０等から取得したデータをフロッピーディスク、メモリカード、ハードディスク等の記憶手段２０に記憶可能とした構成例を示すものである。

【００１４】

プログラム、音声データ、映像データ等のコンテンツは、暗号化処理がなされ、再生手段１０を有するユーザに提供される。正規ユーザは、暗号化データとともに、その暗号化、復号化鍵である鍵データを取得する。

【００１５】

再生手段１０はＣＰＵ１２を有し、入力データの再生処理を再生処理部１４で実行する。再生処理部１４は、暗号化データの復号処理を実行して、提供されたプログラムの再生、音声データ、画像データ等コンテンツ再生を行なう。

【００１６】

正規ユーザは、提供されたプログラムを、再度使用するために記憶手段２０にプログラム／データ等、コンテンツの保存処理を行なう。再生手段１０には、このコンテンツ保存処理を実行するための保存処理部１３を有する。保存処理部１３は、記憶手段２０に記憶されたデータの不正使用を防止するため、データに暗

号化処理を施して保存処理を実行する。

【００１７】

コンテンツを暗号化する際には、コンテンツ暗号用鍵を用いる。保存処理部１３は、コンテンツ暗号用鍵を用いて、コンテンツを暗号化し、それをＦＤ（フロッピーディスク）、メモリカード、ハードディスク等の記憶手段２０の記憶部２１に記憶する。

【００１８】

ユーザは、記憶手段２０から格納コンテンツを取り出して再生する場合には、記憶手段２０から、暗号化データを取り出して、再生手段１０の再生処理部１４において、コンテンツ復号用の鍵、すなわち復号化鍵を用いて復号処理を実行して暗号化データから復号データを取得して再生する。

【００１９】

図１に示す従来の構成例に従えば、フロッピーディスク、メモリカード等の記憶手段２０では格納コンテンツが暗号化されているため、外部からの不正読み出しは防止可能となる。しかしながら、このフロッピーディスクを他のＰＣ、ゲーム機器等の情報機器の再生手段で再生して利用しようとすると、同じコンテンツ鍵、すなわち暗号化されたコンテンツを復号するための同じ復号化鍵を有する再生手段でなければ再生不可能となる。従って、複数の情報機器において利用可能な形態を実現するためには、ユーザに提供する暗号鍵を共通化しておくことが必要となる。

【００２０】

しかしながら、コンテンツの暗号鍵を共通化するということは、正規ライセンスを持たないユーザに暗号処理用の鍵を無秩序に流通させる可能性を高めることになり、正規のライセンスを持たないユーザによるコンテンツの不正利用を防止できなくなるという欠点があり、正規ライセンスを持たないＰＣ、ゲーム機器等での不正利用の排除が困難になる。

【００２１】

さらに、上述のように鍵を共通化した環境においては、例えばあるＰＣ上で作成され、メモリカード、フロッピーデイスク等の記憶手段に保存された暗号化さ

れたコンテンツは、別のフロッピーデイスクに容易に複製することが可能であり、オリジナルのコンテンツデータではなく複製フロッピーデイスクを用いた利用形態が可能となり、ゲーム機器、ＰＣ等の情報機器において利用可能なコンテンツデータが多数複製されたり、または改竄されてしまう可能性があった。

【００２２】

【発明が解決しようとする課題】

コンテンツデータの利用を正当な利用者に限定する手法として認証処理があるが、認証処理と、コンテンツの利用処理とをいかに関連させるか、すなわち、認証処理の手続きをコンテンツの復号処理、または格納処理といかに密接不可分な手続きとして実行させるかについては明確な構成が実現されていない。認証処理についてもパスワードを用いたユーザ認証等は可能であるが記録再生器、あるいは記録デバイス等、機器に対する認証処理とコンテンツ利用処理とを関連付けてコンテンツの不正な利用を排除した構成は実現されていない。

【００２３】

従って例えば、異なる記録再生器において、パスワード入力等によって認証処理を実行すれば、複数の異なる機器においてもコンテンツが利用されてしまい、このようなコンテンツの流用を防止するためには、機器そのそものに対する認証処理とコンテンツ利用処理とを関連付ける処理が必要となる。

【００２４】

本発明は、このような問題点を解決するものであり、本発明の構成においては、記録デバイスにおける認証処理、格納データの暗号処理等を所定のシーケンスにしたがって実行するように規定することにより、機器の認証の実行されていないコンテンツの外部装置からの読み出し等、コンテンツ利用を防止するデータ処理システム、記録デバイス、およびデータ処理方法を提供する。

【００２５】

【課題を解決するための手段】

本発明の第１の側面は、

相互に暗号データの転送を実行する第1の装置と第２の装置とからなるデータ処理システムにおいて、

前記第2の装置は、前記第1の装置との転送データに関する暗号処理を実行する暗号処理部を有し、

該暗号処理部は、

前記第1の装置から転送されるコマンド識別子を予め定められた設定シーケンスにしたがって受領し、該受領コマンド識別子に対応するコマンドをレジスタから取り出して実行させる制御部を有し、

該制御部は、前記第1の装置から転送されるコマンド識別子が前記設定シーケンスと異なるコマンド識別子である場合には、該コマンド識別子に対応するコマンドの処理を中止する構成を有することを特徴とするデータ処理システムにある。

【００２６】

さらに、本発明のデータ処理システムの一実施態様において、前記制御部の有する前記第1の装置から受領するコマンド識別子に関する設定シーケンスは、順次、番号がインクリメントされるコマンド番号設定シーケンスであり、前記制御部は、前記第1の装置からの受領コマンド番号の受付値をメモリに格納するとともに、前記第1の装置からの新規受領コマンド番号を、前記メモリに格納さた受付済みコマンド番号に基づいて設定シーケンスとの一致を判定し、設定シーケンスと異なると判定された場合には、該新規受領コマンド番号に対応するコマンド処理を行なわず、前記メモリに格納したコマンド番号のリセットを実行する構成を有することを特徴とする。

【００２７】

さらに、本発明のデータ処理システムの一実施態様において、前記第2の装置は、前記設定シーケンスに従ったコマンドを格納したコマンドレジスタを有し、前記コマンドレジスタには、前記第1の装置と前記第2の装置との認証処理を実行する認証処理コマンドシーケンスと、前記第1の装置と前記第2の装置との間における転送データに関する暗号処理を実行する暗号処理コマンドシーケンスとが格納されており、前記認証処理コマンドシーケンスに対応するコマンド識別子は、前記暗号処理コマンドシーケンスに対応するコマンド識別子より以前のステップにおいて実行されるようにシーケンス設定がなされていることを特徴とする。

【００２８】

さらに、本発明のデータ処理システムの一実施態様において、前記暗号処理コマンドシーケンスは、前記第1の装置から前記第2の装置に対して転送され、前記第2の装置内の記憶手段に格納される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、または、前記第2の装置内の記憶手段に格納され、前記第２の装置から前記第１の装置に対して転送される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、少なくとも上記いずれかのコマンドシーケンスを含むことを特徴とする。

【００２９】

さらに、本発明のデータ処理システムの一実施態様において、前記制御部は、前記第1の装置と前記第2の装置との認証処理により認証が成立した場合に、認証済みであることを示す認証フラグを設定し、該認証フラグが設定されている間は、前記暗号処理コマンドシーケンスの実行を可能とするコマンド管理制御を実行し、前記制御部は、前記認証処理コマンドシーケンスを新たに実行する際に前記認証フラグをリセットすることを特徴とする。

【００３０】

さらに、本発明のデータ処理システムの一実施態様において、前記制御部は、前記暗号鍵交換処理において、前記設定シーケンスおよびコマンド識別子に基づいてコマンド実行順序を管理し、前記制御部は、前記鍵交換処理に関する一連のコマンド実行中は、前記第1の装置を含む外部装置からの前記設定シーケンスと異なるコマンド処理を受け付けない構成であることを特徴とする。

【００３１】

さらに、本発明のデータ処理システムの一実施態様において、前記第2の装置は、暗号化データを記憶するデータ記憶部を有する記憶デバイスであり、前記第1の装置は、前記記憶デバイスに対するデータの格納処理、および前記記憶デバイスに格納されたデータを取り出して再生、実行を行なう記録再生器であり、前記記録再生器は、前記記録デバイスとの転送データの暗号処理を実行する暗号処理部を有することを特徴とする。

【００３２】

さらに、本発明のデータ処理システムの一実施態様において、前記記録デバイスは、前記記録再生器と記録デバイス間の認証処理に適用する認証鍵、および前記記録デバイス内のデータ記憶部に格納するデータの暗号化鍵としての保存鍵を格納した鍵ブロックを有し、前記記録デバイスの暗号処理部における前記制御部は、前記記録再生器から前記設定シーケンスにしたがってコマンド識別子を受領して前記鍵ブロックに格納した認証鍵を用いた認証処理を実行し、該認証処理完了後に前記保存鍵を用いた鍵交換処理を伴うデータの暗号処理を実行する構成であることを特徴とする。

【００３３】

さらに、本発明のデータ処理システムの一実施態様において、前記鍵ブロックは、それぞれ異なる認証鍵および保存鍵を格納した複数の鍵ブロックから構成され、前記記録再生器は、前記複数の鍵ブロックから、認証処理およびデータの暗号処理に使用する１つの鍵ブロックを指定鍵ブロックとして前記記録デバイスに通知し、前記記録デバイスは、指定鍵ブロックに格納された認証鍵を用いた認証処理、および保存鍵を用いたデータの暗号処理を実行する構成であることを特徴とする。

【００３４】

さらに、本発明の第２の側面は、

外部装置との間で転送可能なコンテンツデータを記憶するデータ記憶部を有する記録デバイスであり、

前記記録デバイスは、外部装置との転送データに関する暗号処理を実行する暗号処理部を有し、

該暗号処理部は、

外部装置から転送されるコマンド識別子を予め定められた設定シーケンスにしたがって受領し、該受領コマンド識別子に対応するコマンドをレジスタから取り出して実行させる制御部を有し、

該制御部は、前記外部装置から転送されるコマンド識別子が前記設定シーケンスと異なるコマンド識別子である場合には、該コマンド識別子に対応するコマンドの処理を中止する構成を有することを特徴とする記録デバイスにある。

【００３５】

さらに、本発明の記録デバイスの一実施態様において、前記制御部は、前記設定シーケンスとして、順次、番号がインクリメントされるコマンド番号設定シーケンスを有し、前記制御部は、前記外部装置からの受領コマンド番号の受付値をメモリに格納するとともに、前記外部装置からの新規受領コマンド番号を、前記メモリに格納さた受付済みコマンド番号に基づいて設定シーケンスとの一致を判定し、設定シーケンスと異なると判定された場合には、該新規受領コマンド番号に対応するコマンド処理を行なわず、前記メモリに格納したコマンド番号のリセットを実行する構成を有することを特徴とする。

【００３６】

さらに、本発明の記録デバイスの一実施態様において、前記記録デバイスは、前記設定シーケンスに従ったコマンドを格納したコマンドレジスタを有し、前記コマンドレジスタには、前記外部装置と前記記録デバイスとの認証処理を実行する認証処理コマンドシーケンスと、前記外部装置と前記記録デバイスとの間における転送データに関する暗号処理を実行する暗号処理コマンドシーケンスとが格納されており、前記認証処理コマンドシーケンスに対応するコマンド識別子は、前記暗号処理コマンドシーケンスに対応するコマンド識別子より以前のステップにおいて実行されるようにシーケンス設定がなされていることを特徴とする。

【００３７】

さらに、本発明の記録デバイスの一実施態様において、前記暗号処理コマンドシーケンスは、前記外部装置から前記記録デバイスに対して転送され、前記記録デバイス内の記憶手段に格納される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、または、前記記録デバイス内の記憶手段に格納され、前記記録デバイスから前記外部装置に対して転送される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、少なくとも上記いずれかのコマンドシーケンスを含むことを特徴とする。

【００３８】

さらに、本発明の記録デバイスの一実施態様において、前記制御部は、前記外部装置と前記記録デバイスとの認証処理により認証が成立した場合に、認証済み

であることを示す認証フラグを設定し、該認証フラグが設定されている間は、前記暗号処理コマンドシーケンスの実行を可能とするコマンド管理制御を実行し、前記制御部は、前記認証処理コマンドシーケンスを新たに実行する際に前記認証フラグをリセットすることを特徴とする。

【００３９】

さらに、本発明の記録デバイスの一実施態様において、前記制御部は、前記暗号鍵交換処理において、前記設定シーケンスおよびコマンド識別子に基づいてコマンド実行順序を管理し、前記制御部は、前記鍵交換処理に関する一連のコマンド実行中は、前記外部装置を含む外部装置からの前記設定シーケンスと異なるコマンド処理を受け付けない構成であることを特徴とする。

【００４０】

さらに、本発明の記録デバイスの一実施態様において、前記記録デバイスは、前記外部装置と記録デバイス間の認証処理に適用する認証鍵、および前記記録デバイス内のデータ記憶部に格納するデータの暗号化鍵としての保存鍵を格納した鍵ブロックを有し、前記記録デバイスの暗号処理部における前記制御部は、前記外部装置から前記設定シーケンスにしたがってコマンド識別子を受領して前記鍵ブロックに格納した認証鍵を用いた認証処理を実行し、該認証処理完了後に前記保存鍵を用いた鍵交換処理を伴うデータの暗号処理を実行する構成であることを特徴とする。

【００４１】

さらに、本発明の記録デバイスの一実施態様において、前記鍵ブロックは、それぞれ異なる認証鍵および保存鍵を格納した複数の鍵ブロックから構成され、前記外部装置は、前記複数の鍵ブロックから、認証処理およびデータの暗号処理に使用する１つの鍵ブロックを指定鍵ブロックとして前記記録デバイスに通知し、前記記録デバイスは、指定鍵ブロックに格納された認証鍵を用いた認証処理、および保存鍵を用いたデータの暗号処理を実行する構成であることを特徴とする。

【００４２】

さらに、本発明の第３の側面は、

相互に暗号データの転送を実行する第1の装置と第２の装置とからなるデータ

処理システムにおけるデータ処理方法であり、

前記第2の装置は、

前記第1の装置から転送されるコマンド識別子を予め定められた設定シーケンスにしたがって受領し、該受領コマンド識別子に対応するコマンドをレジスタから取り出して実行させるコマンド処理制御ステップを実行し、

前記コマンド処理制御において、前記第1の装置から転送されるコマンド識別子が前記設定シーケンスと異なるコマンド識別子である場合には、該コマンド識別子に対応するコマンドの処理を中止することを特徴とするデータ処理方法にある。

【００４３】

さらに、本発明のデータ処理方法の一実施態様において、前記コマンド処理制御ステップにおいて、前記第1の装置から受領するコマンド識別子に関する設定シーケンスは、順次、番号がインクリメントされるコマンド番号設定シーケンスであり、前記コマンド処理制御ステップは、前記第1の装置からの受領コマンド番号の受付値をメモリに格納するステップと、前記第1の装置からの新規受領コマンド番号を、前記メモリに格納さた受付済みコマンド番号に基づいて設定シーケンスとの一致を判定する判定ステップと、前記判定ステップにおいて、設定シーケンスと異なると判定された場合には、該新規受領コマンド番号に対応するコマンド処理を行なわず、前記メモリに格納したコマンド番号のリセットを実行することを特徴とする。

【００４４】

さらに、本発明のデータ処理方法の一実施態様において、前記データ処理方法において、前記コマンド処理制御ステップは、前記第1の装置と前記第2の装置との認証処理を実行する認証処理コマンドシーケンスと、前記第1の装置と前記第2の装置との間における転送データに関する暗号処理を実行する暗号処理コマンドシーケンスとを、実行するステップであり、前記設定シーケンスは、前記認証処理コマンドシーケンスを前記暗号処理コマンドシーケンスに先行して実行するシーケンスであることを特徴とする。

【００４５】

さらに、本発明のデータ処理方法の一実施態様において、前記暗号処理コマンドシーケンスは、前記第1の装置から前記第2の装置に対して転送され、前記第2の装置内の記憶手段に格納される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、または、前記第2の装置内の記憶手段に格納され、前記第２の装置から前記第１の装置に対して転送される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、少なくとも上記いずれかのコマンドシーケンスを含むことを特徴とする。

【００４６】

さらに、本発明のデータ処理方法の一実施態様において、前記第1の装置と前記第2の装置との認証処理により認証が成立した場合に認証済みであることを示す認証フラグを設定する認証フラグ設定ステップを含み、前記コマンド処理制御ステップは、前記認証フラグが設定されている間は、前記暗号処理コマンドシーケンスの実行を可能とするコマンド管理制御を実行することを特徴とする。

【００４７】

さらに、本発明のデータ処理方法の一実施態様において、前記認証処理コマンドシーケンスを新たに実行する際に前記認証フラグをリセットすることを特徴とする。

【００４８】

さらに、本発明のデータ処理方法の一実施態様において、前記データ処理方法における前記コマンド処理制御ステップにおいて、前記鍵交換処理に関する一連のコマンド実行中は、前記設定シーケンスおよびコマンド識別子に基づいてコマンド実行順序を管理し、

前記第1の装置を含む外部装置からの前記設定シーケンスと異なるコマンド処理を受け付けないことを特徴とする。

【００４９】

さらに、本発明の第４の側面は、

相互に暗号データの転送を実行する第1の装置と第２の装置とからなるデータ処理システムにおけるデータ処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、

前記第1の装置から前記第2の装置に転送されるコマンド識別子を予め定められた設定シーケンスにしたがって受領し、該受領コマンド識別子に対応するコマンドをレジスタから取り出して実行させるコマンド処理制御ステップを有し、

前記コマンド処理制御ステップにおいて、前記第1の装置から転送されるコマンド識別子が前記設定シーケンスと異なるコマンド識別子である場合には、該コマンド識別子に対応するコマンドの処理を中止するステップを含むことを特徴とするプログラム提供媒体にある。

【００５０】

本発明に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯなどの記憶媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【００５１】

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【００５２】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００５３】

【発明の実施の形態】

以下に本発明の実施の形態を説明する。説明の手順は、以下の項目に従って行なう。

（１）データ処理装置構成

（２）コンテンツデータフォーマット

（３）データ処理装置において適用可能な暗号処理概要

（４）記録再生器の格納データ構成

（５）記録デバイスの格納データ構成

（６）記録再生器、記録デバイス間における相互認証処理

（６－１）相互認証処理の概要

（６－２）相互認証時の鍵ブロックの切り替え

（７）記録再生器から記録デバイスへのダウンロード処理

（８）記録デバイス格納情報の記録再生器での再生処理

（９）相互認証後の鍵交換処理

（１０）複数のコンテンツデータフォーマットと、各フォーマットに対応するダウンロードおよび再生処理

（１１）コンテンツプロバイダにおけるチェック値（ＩＣＶ）生成処理態様

（１２）マスタ鍵に基づく暗号処理鍵生成構成

（１３）暗号処理における暗号強度の制御

（１４）コンテンツデータにおける取扱方針中の起動優先順位に基づくプログラム起動処理

（１５）コンテンツ構成および再生(伸長)処理

（１６）セーブデータの生成および記録デバイスへの格納、再生処理

（１７）不正機器の排除（リボケーション）構成

（１８）セキュアチップ構成および製造方法

【００５４】

（１）データ処理装置構成

図２に本発明のデータ処理装置の一実施例に係る全体構成ブロック図を示す。本発明のデータ処理装置は、記録再生器３００と記録デバイス４００とを主要構成要素とする。

【００５５】

記録再生器３００は、例えばパーソナル・コンピュータ（ＰＣ：Personal Computer）、あるいはゲーム機器等によって構成される。記録再生器３００は、図２に示すように、記録再生器３００における暗号処理時の記録デバイス４００と

の通信制御を含む統括的制御を実行する制御部３０１、暗号処理全般を司る記録再生器暗号処理部３０２、記録再生器に接続される記録デバイス４００と認証処理を実行しデータの読み書きを行う記録デバイスコントローラ３０３、ＤＶＤなどのメディア５００から少なくともデータの読み出しを行う読み取り部３０４、外部とデータの送受信を行う通信部３０５を有する。

【００５６】

記録再生器３００は、制御部３０１の制御により記録デバイス４００に対するコンテンツデータのダウンロード、記録デバイス４００からのコンテンツデータ再生を実行する。記録デバイス４００は、記録再生器３００に対して好ましくは着脱可能な記憶媒体、例えばメモリカード等であり、ＥＥＰＲＯＭ、フラッシュメモリ等の不揮発メモリ、ハードディスク、電池つきＲＡＭなどによって構成される外部メモリ４０２を有する。

【００５７】

記録再生器３００は、図２の左端に示す記憶媒体、ＤＶＤ、ＣＤ、ＦＤ、ＨＤＤに格納されたコンテンツデータを入力可能なインタフェースとしての読み取り部３０４、インターネット等のネットワークから配信されるコンテンツデータを入力可能なインタフェースとしての通信部３０５を有し、外部からコンテンツを入力する。

【００５８】

記録再生器３００は、暗号処理部３０２を有し、読取部３０４または通信部３０５を介して外部から入力されるコンテンツデータを記録デバイス４００にダウンロード処理する際、あるいはコンテンツデータを記録デバイス４００から再生、実行する際の認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する。暗号処理部３０２は、暗号処理部３０２全体を制御する制御部３０６、暗号処理用の鍵などの情報を保持し、外部から容易にデータを読み出せないように処理が施された内部メモリ３０７、暗号化処理、復号化処理、認証用のデータの生成・検証、乱数の発生などを行う暗号／復号化部３０８から構成されている。

【００５９】

制御部３０１は、例えば、記録再生器３００に記録デバイス４００が装着された際に記録デバイスコントローラ３０３を介して記録デバイス４００に初期化命令を送信したり、あるいは、記録再生器暗号処理部３０２の暗号／復号化部３０８と記録デバイス暗号処理部４０１の暗号／復号化部４０６の間で行われる相互認証処理、チェック値照合処理、暗号化、復号化処理等、各種処理における仲介処理を行なう。これらの各処理については、後段で詳細に説明する。

【００６０】

暗号処理部３０２は、前述のように認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する処理部であり、暗号処理制御部３０６、内部メモリ３０７、暗号／復号化部３０８を有する。

【００６１】

暗号処理制御部３０６は、記録再生器３００において実行される認証処理、暗号化／復号化処理等の暗号処理全般に関する制御を実行する制御部であり、例えば、記録再生器３００と記録デバイス４００との間で実行される認証処理の完了時における認証完了フラグの設定、記録再生器暗号処理部３０２の暗号／復号化部３０８において実行される各種処理、例えばダウンロード、あるいは再生コンテンツデータに関するチェック値生成処理の実行命令、各種鍵データの生成処理の実行命令等、暗号処理全般に関する制御を行なう。

【００６２】

内部メモリ３０７は、後段で詳細に説明するが、記録再生器３００において実行される相互認証処理、チェック値照合処理、暗号化、復号化処理等、各種処理において必要となる鍵データ、あるいは識別データ等を格納する。

【００６３】

暗号／復号化部３０８は、内部メモリ３０７に格納された鍵データ等を使用して、外部から入力されるコンテンツデータを記録デバイス４００にダウンロード処理する際、あるいは記録デバイス４００に格納されたコンテンツデータを記録デバイス４００から再生、実行する際の認証処理、暗号化処理、復号化処理、さらに所定のチェック値や電子署名の生成・検証、データの検証、乱数の発生などの処理を実行する。

【００６４】

ここで、記録再生器暗号処理部３０２の内部メモリ３０７は、暗号鍵などの重要な情報を保持しているため、外部から不正に読み出しにくい構造にしておく必要がある。従って、暗号処理部３０２は、外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニュウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または／かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性を有する耐タンパメモリとして構成される。この構成については、後段で詳細に説明する。

【００６５】

記録再生器３００は、これらの暗号処理機能の他に、中央演算処理装置（メインＣＰＵ：Central Processing Unit）１０６、ＲＡＭ（Random Access Memory）１０７、ＲＯＭ(Read Only Memory)１０８、ＡＶ処理部１０９、入力インタフェース１１０、ＰＩＯ（パラレルＩ／Ｏインタフェース）１１１、ＳＩＯ（シリアルＩ／Ｏインタフェース）１１２を備えている。

【００６６】

中央演算処理装置（メインＣＰＵ：Central Processing Unit）１０６、ＲＡＭ（Random Access Memory）１０７、ＲＯＭ(Read Only Memory)１０８は、記録再生器３００本体の制御系として機能する構成部であり、主として記録再生器暗号処理部３０２で復号されたデータの再生を実行する再生処理部として機能する。例えば中央演算処理装置（メインＣＰＵ：Central Processing Unit）１０６は、制御部３０１の制御のもとに記録デバイスから読み出されて復号されたコンテンツデータをＡＶ処理部１０９へ出力する等、コンテンツの再生、実行に関する制御を行なう。

【００６７】

ＲＡＭ１０７は、ＣＰＵ１０６における各種処理用の主記憶メモリとして使用され、メインＣＰＵ１０６による処理のための作業領域として使用される。ＲＯＭ１０８は、メインＣＰＵ１０６で起動されるＯＳ等を立ち上げるための基本プログラム等が格納される。

【００６８】

ＡＶ処理部１０９は、具体的には、例えばＭＰＥＧ２デコーダ、ＡＴＲＡＣデコーダ、ＭＰ３デコーダ等のデータ圧縮伸長処理機構を有し、記録再生器本体に付属または接続された図示しないディスプレイまたはスピーカ等のデータ出力機器に対するデータ出力のための処理を実行する。

【００６９】

入力インタフェース１１０は、接続されたコントローラ、キーボード、マウス等、各種の入力手段からの入力データをメインＣＰＵ１０６に出力する。メインＣＰＵ１０６は、例えば実行中のゲームプログラム等に基づいて使用者からのコントローラからの指示に従った処理を実行する。

【００７０】

ＰＩＯ（パラレルＩ／Ｏインタフェース）１１１、ＳＩＯ（シリアルＩ／Ｏインタフェース）１１２は、メモリカード、ゲームカートリッジ等の記憶装置、携帯用電子機器等との接続インタフェースとして使用される。

【００７１】

また、メインＣＰＵ１０６は、例えば実行中のゲーム等に関する設定データ等をセーブデータとして記録デバイス４００に記憶する際の制御も行なう。この処理の際には、記憶データを制御部３０１に転送し、制御部３０１は必要に応じて暗号処理部３０２にセーブデータに関する暗号処理を実行させ、暗号化データを記録デバイス４００に格納する。これらの暗号処理については、後段で詳細に説明する。

【００７２】

記録デバイス４００は、前述したように好ましくは記録再生器３００に対して着脱可能な記憶媒体であり、例えばメモリカードによって構成される。記録デバイス４００は暗号処理部４０１、外部メモリ４０２を有する。

【００７３】

記録デバイス暗号処理部４０１は、記録再生器３００からのコンテンツデータのダウンロード、または記録デバイス４００から記録再生器３００へのコンテンツデータの再生処理時等における記録再生器３００と記録デバイス４００間の相

互認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する処理部であり、記録再生器３００の暗号処理部と同様、制御部、内部メモリ、暗号／復号化部等を有する。これらの詳細は図３に示す。外部メモリ４０２は、前述したように、例えばＥＥＰＲＯＭ等のフラッシュメモリからなる不揮発メモリ、ハードディスク、電池つきＲＡＭなどによって構成され、暗号化されたコンテンツデータ等を格納する。

【００７４】

図３は、本発明のデータ処理装置がデータ供給を受けるコンテンツ提供手段であるメディア５００、通信手段６００から入力されるデータ構成の概略を示すとともに、これらコンテンツ提供手段５００，６００からコンテンツを入力する記録再生器３００と、記録デバイス４００における暗号処理に関する構成を中心として、その構成を示した図である。

【００７５】

メディア５００は、例えば光ディスクメディア、磁気ディスクメディア、磁気テープメディア、半導体メディア等である。通信手段６００は、インターネット通信、ケーブル通信、衛星通信等の、データ通信可能な手段である。

【００７６】

図３において、記録再生器３００は、コンテンツ提供手段であるメディア５００、通信手段６００から入力されるデータ、すなわち図３に示すような所定のフォーマットに従ったコンテンツを検証し、検証後にコンテンツを記録デバイス４００に保存する。

【００７７】

図３のメディア５００、通信手段６００部分に示すようにコンテンツデータは以下のような構成部を有する。

識別情報：コンテンツデータの識別子としての識別情報。

取扱方針：コンテンツデータの構成情報、例えばコンテンツデータを構成するヘッダー部サイズ、コンテンツ部サイズ、フォーマットのバージョン、コンテンツがプログラムかデータか等を示すコンテンツタイプ、さらにコンテンツがダウンロードした機器だけでしか利用できないのか他の機器でも利用できるのか等の

利用制限情報等を含む取扱方針。

ブロック情報：コンテンツブロックの数、ブロックサイズ、暗号化の有無を示す暗号化フラグ等から構成されるブロック情報。

鍵データ：上述のブロック情報を暗号化する暗号化鍵、あるいはコンテンツブロックを暗号化するコンテンツ鍵等からなる鍵データ。

コンテンツブロック：実際の再生対象となるプログラムデータ、音楽、画像データ等からなるコンテンツブロック。

を有する。なお、コンテンツデータ詳細については、後段で図４以下を用いてさらに詳細に説明する。

【００７８】

コンテンツデータは、コンテンツ鍵（ここでは、これをコンテンツ鍵（Content Key（以下、Ｋｃｏｎとする））と呼ぶ）によって暗号化されて、メディア５００、通信手段６００から記録再生器３００に提供される。コンテンツは、記録再生器３００を介して記録デバイス４００の外部メモリに格納することができる。

【００７９】

例えば、記録デバイス４００は、記録デバイス内の内部メモリ４０５に格納された記録デバイス固有の鍵（ここでは、これを保存鍵（Storage Key（以下、Ｋｓｔｒとする））と呼ぶ）を用いて、コンテンツデータに含まれるコンテンツ、及びコンテンツデータのヘッダ情報として含まれるブロック情報、各種鍵情報、例えばコンテンツ鍵Ｋｃｏｎなどを暗号化して外部メモリ４０２に記憶する。コンテンツデータの記録再生器３００から記録デバイス４００へのダウンロード処理、あるいは記録再生器３００による記録デバイス４００内に格納されたコンテンツデータの再生処理においては、機器間の相互認証処理、コンテンツデータの暗号化、復号化処理等、所定の手続きが必要となる。これらの処理については、後段で詳細に説明する。

【００８０】

記録デバイス４００は、図３に示すように暗号処理部４０１、外部メモリ４０２を有し、暗号処理部４０１は、制御部４０３、通信部４０４、内部メモリ４０

５、暗号／復号化部４０６、外部メモリ制御部４０７を有する。

【００８１】

記録デバイス４００は、暗号処理全般を司り、外部メモリ４０２を制御するとともに、記録再生器３００からのコマンドを解釈し、処理を実行する記録デバイス暗号処理部４０１と、コンテンツなどを保持する外部メモリ４０２からなる。

【００８２】

記録デバイス暗号処理部４０１は、記録デバイス暗号処理部４０１全体を制御する制御部４０３、記録再生器３００とデータの送受信を行う通信部４０４、暗号処理用の鍵データなどの情報を保持し、外部から容易に読み出せないように処理が施された内部メモリ４０５、暗号化処理、復号化処理、認証用のデータの生成・検証、乱数の発生などを行う暗号／復号化部４０６、外部メモリ４０２のデータを読み書きする外部メモリ制御部４０７を有する。

【００８３】

制御部４０３は、記録デバイス４００において実行される認証処理、暗号化／復号化処理等の暗号処理全般に係る制御を実行する制御部であり、例えば、記録再生器３００と記録デバイス４００との間で実行される認証処理の完了時における認証完了フラグの設定、暗号処理部４０１の暗号／復号化部４０６において実行される各種処理、例えばダウンロード、あるいは再生コンテンツデータに関するチェック値生成処理の実行命令、各種鍵データの生成処理の実行命令等、暗号処理全般に関する制御を行なう。

【００８４】

内部メモリ４０５は、後段で詳細に説明するが、複数のブロックを持つメモリによって構成されており、記録デバイス４００において実行される相互認証処理、チェック値照合処理、暗号化、復号化処理等、各種処理において必要となる鍵データ、あるいは識別データ等の組を複数格納した構成となっている。

【００８５】

記録デバイス暗号処理部４０１の内部メモリ４０５は、先に説明した記録再生器暗号処理部３０２の内部メモリ３０７と同様、暗号鍵などの重要な情報を保持しているため、外部から不正に読み出しにくい構造にしておく必要がある。従っ

て、記録デバイス４００の暗号処理部４０１は、外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニュウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または／かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性とした構成とされる。なお、記録再生器暗号処理部３０２は、鍵などの秘密の情報を容易に外部に漏らさないように構成されたソフトウェアであってもよい。

【００８６】

暗号／復号化部４０６は、記録再生器３００からのコンテンツデータのダウンロード処理、記録デバイス４００の外部メモリ４０２に格納されたコンテンツデータの再生処理、あるいは、記録再生器３００と記録デバイス４００間の相互認証処理の際、内部メモリ４０５に格納された鍵データ等を使用して、データの検証処理、暗号化処理、復号化処理、所定のチェック値や電子署名の生成・検証、乱数の発生などの処理等を実行する。

【００８７】

通信部４０４は、記録再生器３００の記録デバイスコントローラ３０３に接続され、記録再生器３００の制御部３０１、あるいは、記録デバイス４０３の制御部４０３の制御に従って、コンテンツデータのダウンロード処理、再生処理、あるいは、相互認証処理の際の記録再生器３００と記録デバイス４００間の転送データの通信を行なう。

【００８８】

（２）コンテンツデータフォーマット

次に、図４乃至図６を用いて、本発明のシステムにおけるメディア５００に格納され、またはデータ通信手段６００上を流通するデータのデータフォーマットについて説明する。

【００８９】

図４に示す構成がコンテンツデータ全体のフォーマットを示す図であり、図５に示す構成がコンテンツデータのヘッダ部の一部を構成する「取扱方針」の詳細を示す図であり、図６に示す構成がコンテンツデータのヘッダ部の一部を構成する「ブロック情報」の詳細を示す図である。

【００９０】

なお、ここでは、本発明のシステムにおいて適用されるデータフォーマットの代表的な一例について説明するが、本発明のシステムでは、例えばゲームプログラムに対応したフォーマット、音楽データ等のリアルタイム処理に適したフォーマット等、異なる複数のデータフォーマットが利用可能であり、これらのフォーマットの態様については、後段「（１０）複数のコンテンツデータフォーマットと、各フォーマットに対応するダウンロードおよび再生処理」において、さらに詳しく述べる。

【００９１】

図４に示すデータフォーマットにおいて、グレーで示す部分は暗号化されたデータであり、二重枠の部分は改竄チェックデータ、その他の白い部分は暗号化されていない平文のデータである。暗号化部の暗号化鍵は、それぞれの枠の左に示す鍵である。図４に示す例においては、コンテンツ部の各ブロック（コンテンツブロックデータ）に暗号化されたものと暗号化されていないものとが混在している。これらの形態は、コンテンツデータに応じて異なるものであり、データに含まれるすべてのコンテンツブロックデータが暗号化されている構成であってもよい。

【００９２】

図４に示すように、データフォーマットは、ヘッダー部とコンテンツ部に分かれており、ヘッダー部は、識別情報（Content ＩＤ）、取扱方針（Usage Policy）、チェック値Ａ（Integrity Check Value A（以下、ＩＣＶａとする））、ブロック情報鍵（Block Information Table Key（以下、Ｋｂｉｔとする））、コンテンツ鍵Ｋｃｏｎ、ブロック情報（Block Information Table（以下、ＢＩＴとする））、チェック値Ｂ（ＩＣＶｂ）、総チェック値（ＩＣＶｔ）により構成されており、コンテンツ部は、複数のコンテンツブロック（例えば暗号化されたコンテンツと、暗号化されていないコンテンツ）から構成されている。

【００９３】

ここで、識別情報は、コンテンツを識別するための個別の識別子（Ｃｏｎｔｅｎｔ ＩＤ）を示している。取扱方針は、図５にその詳細を示すように、ヘッダ

一部分のサイズを示すヘッダーサイズ（Header Length）、コンテンツ部分のサイズを示すコンテンツサイズ（Content Length）、フォーマットのバージョン情報を示すフォーマットバージョン（Format Version）、フォーマットの種類を示すフォーマットタイプ（Format Type）、コンテンツ部に保存されているコンテンツがプログラムなのか、データなのか等コンテンツの種類を示すコンテンツタイプ（Content Type）、コンテンツタイプがプログラムである場合の起動優先順位を示す起動優先順位情報（Operation Priority）、このフォーマットに従ってダウンロードされたコンテンツが、ダウンロードした機器だけでしか利用できないのか、他の同様な機器でも利用できるのかを示す利用制限情報（Localization Field）、このフォーマットに従ってダウンロードされたコンテンツが、ダウンロードした機器から他の同様な機器に複製できるのか否かを示す複製制限情報（Copy Permission）、このフォーマットに従ってダウンロードされたコンテンツが、ダウンロードした機器から他の同様な機器に移動できるのか否かを示す移動制限情報（Move Permission）、コンテンツ部内のコンテンツブロックを暗号するのに使用したアルゴリズムを示す暗号アルゴリズム（Encryption Algorithm）、コンテンツ部内のコンテンツを暗号化するのに使用したアルゴリズムの使用方法を示す暗号化モード（Encryption Mode）、チェック値の生成方法を示す検証方法（Integrity Check Method）から構成されている。

【００９４】

なお、上述した取扱方針に記録するデータ項目は、１つの例であり、対応するコンテンツデータの態様に応じて様々な取扱方針情報を記録することが可能である。例えば後段の「（１７）不正機器の排除（リボケーション）構成」で詳しく述べるが、不正な記録再生器の識別子をデータとして記録して、利用開始時の照合によって不正機器によるコンテンツ利用を排除するように構成することも可能である。

【００９５】

チェック値Ａ，ＩＣＶａは、識別情報、取扱方針の改竄を検証するためのチェック値である。コンテンツデータ全体ではなく部分データのチェック値、すなわち部分チェック値として機能する。データブロック情報鍵Ｋｂｉｔは、ブロック

情報を暗号化するのに用いられ、コンテンツ鍵Ｋｃｏｎは、コンテンツブロックを暗号化するのに用いられる。なお、ブロック情報鍵Ｋｂｉｔ及びコンテンツ鍵Ｋｃｏｎは、メディア５００上および通信手段６００上では後述する配送鍵（Distribution Key（以下、Ｋｄｉｓとする））で暗号化されている。

【００９６】

ブロック情報の詳細を図６に示す。なお、図６のブロック情報は、図４から理解されるようにすべてブロック情報鍵Ｋｂｉｔによって暗号化されているデータである。ブロック情報は、図６に示すように、コンテンツブロックの数を示すコンテンツブロック数（Block Number）とＮ個のコンテンツブロック情報から構成されている。コンテンツブロック情報は、ブロックサイズ（Block Length）、暗号化されているか否かを示す暗号化フラグ（Encryption Flag）、チェック値を計算する必要があるか否かを示す検証対象フラグ（ＩＣＶ Flag）、コンテンツチェック値（ＩＣＶｉ）から構成されている。

【００９７】

コンテンツチェック値は、各コンテンツブロックの改竄を検証するために用いられるチェック値である。コンテンツチェック値の生成手法の具体例については、後段の「（１０）複数のデータフォーマットと、各フォーマットに対応する記録デバイスへのダウンロード処理および記録デバイスからの再生処理」の欄で説明する。なお、ブロック情報を暗号化しているブロック情報鍵Ｋｂｉｔは、さらに、配送鍵Ｋｄｉｓによって暗号化されている。

【００９８】

図４のデータフォーマットの説明を続ける。チェック値Ｂ，ＩＣＶｂは、ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎ、ブロック情報の改竄を検証するためのチェック値である。コンテンツデータ全体ではなく部分データのチェック値、すなわち部分チェック値として機能する。総チェック値ＩＣＶｔは、ＩＣＶａ、ＩＣＶｂ、各コンテンツブロックのチェック値ＩＣＶｉ（設定されている場合）、これらの部分チェック値、あるいはそのチェック対象となるデータ全ての改竄を検証するためのチェック値である。

【００９９】

なお、図６においては、ブロックサイズ、暗号化フラグ、検証対象フラグを自由に設定できるようにしているが、ある程度ルールを決めた構成としてもよい。例えば、暗号文領域と平文領域を固定サイズ繰り返しにしたり、全コンテンツデータを暗号化したりし、ブロック情報ＢＩＴを圧縮してもよい。また、コンテンツ鍵Ｋｃｏｎをコンテンツブロック毎に異なるようにするため、コンテンツ鍵Ｋｃｏｎをヘッダー部分ではなく、コンテンツブロックに含ませるようにしてもよい。コンテンツデータフォーマットの例については、「（１０）複数のコンテンツデータフォーマットと、各フォーマットに対応するダウンロードおよび再生処理」の項目において、さらに詳細に説明する。

【０１００】

（３）本発明のデータ処理装置において適用可能な暗号処理概要

次に、本発明のデータ処理装置において適用され得る各種暗号処理の態様について説明する。なお、本項目「（３）本発明のデータ処理装置において適用可能な暗号処理の概要」に示す暗号処理に関する説明は、後段で具体的に説明する本発明のデータ処理装置における各種処理、例えばａ．記録再生器と記録デバイス間での認証処理。ｂ．コンテンツの記録デバイスに対するダウンロード処理。ｃ．記録デバイスに格納したコンテンツの再生処理等の処理において実行される処理の基礎となる暗号処理の態様について、その概要を説明するものである。記録再生器３００と記録デバイス４００における具体的処理については、本明細書の項目（４）以下において、各処理毎に詳細に説明する。

【０１０１】

以下、データ処理装置において適用可能な暗号処理の概要について、

（３－１）共通鍵暗号方式によるメッセージ認証

（３－２）公開鍵暗号方式による電子署名

（３－３）公開鍵暗号方式による電子署名の検証

（３－４）共通鍵暗号方式による相互認証

（３－５）公開鍵証明書

（３－６）公開鍵暗号方式による相互認証

（３－７）楕円曲線暗号を用いた暗号化処理

（３－８）楕円曲線暗号を用いた復号化処理

（３－９）乱数生成処理

の順に説明する。

【０１０２】

（３－１）共通鍵暗号方式によるメッセージ認証

まず、共通鍵暗号方式を用いた改竄検出データの生成処理について説明する。改竄検出データは、改竄の検出を行ないたいデータに付け、改竄のチェックおよび作成者認証をするためのデータである。

【０１０３】

例えば、図４で説明したデータ構造中の二重枠部分の各チェック値Ａ，Ｂ、総チェック値、および図６に示すブロック情報中の各ブロックに格納されたコンテンツチェック値等が、この改竄検出データとして生成される。

【０１０４】

ここでは、電子署名データの生成処理方法の例の１つとして共通鍵暗号方式におけるＤＥＳを用いた例を説明する。なお、本発明においては、ＤＥＳ以外にも、同様の共通鍵暗号方式における処理として例えばＦＥＡＬ（Fast Enciphermen t ALgorithm：NTT）、ＡＥＳ（Advanced Encryption Standard：米国次期標準暗号）等を用いることも可能である。

【０１０５】

一般的なＤＥＳを用いた電子署名の生成方法を図７を用いて説明する。まず、電子署名を生成するに先立ち、電子署名の対象となるメッセージを８バイト単位に分割する（以下、分割されたメッセージをＭ１、Ｍ２、・・・、ＭＮとする）。そして、初期値（Initial Value（以下、ＩＶとする））とＭ１を排他的論理和する（その結果をＩ１とする）。次に、Ｉ１をＤＥＳ暗号化部に入れ、鍵（以下、Ｋ１とする）を用いて暗号化する（出力をＥ１とする）。続けて、Ｅ１およびＭ２を排他的論理和し、その出力Ｉ２をＤＥＳ暗号化部へ入れ、鍵Ｋ１を用いて暗号化する（出力Ｅ２）。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたＥＮが電子署名になる。この値は一般にはメッセージ認証符号（ＭＡＣ（Message Authentication Code））と呼ばれ、メッ

セージの改竄チェックに用いられる。また、このように暗号文を連鎖させる方式のことをＣＢＣ（Cipher Block Chaining）モードと呼ぶ。

【０１０６】

なお、図７のような生成例において出力されるＭＡＣ値が、図４で示すデータ構造中の二重枠部分の各チェック値Ａ，Ｂ、総チェック値、および図６に示すブロック情報中の各ブロックに格納されたコンテンツチェック値ＩＣＶ１～ＩＣＶＮとして使用可能である。このＭＡＣ値の検証時には、検証者が生成時と同様の方法でＭＡＣ値を生成し、同一の値が得られた場合、検証成功とする。

【０１０７】

なお、図７に示す例では初期値ＩＶを、初めの８バイトメッセージＭ１に排他的論理和したが、初期値ＩＶ＝０として、初期値を排他的論理和しない構成とすることも可能である。

【０１０８】

図７に示すＭＡＣ値生成方法に対して、さらにセキュリティを向上させたＭＡＣ値生成方法を示す処理構成図を図８に示す。図８は、図７のシングルＤＥＳに代えてトリプルＤＥＳ（Triple ＤＥＳ）を用いてＭＡＣ値の生成を実行する例を示したものである。

【０１０９】

図８に示す各トリプルＤＥＳ（Triple ＤＥＳ）構成部の詳細構成例を図９に示す。図９（ａ）、（ｂ）に示すようにトリプルＤＥＳ（Triple ＤＥＳ）としての構成には２つの異なる態様がある。図９（ａ）は、２つの暗号鍵を用いた例を示すものであり、鍵１による暗号化処理、鍵２による復号化処理、さらに鍵１による暗号化処理の順に処理を行う。鍵は、Ｋ１、Ｋ２、Ｋ１の順に２種類用いる。図９（ｂ）は３つの暗号鍵を用いた例を示すものであり、鍵１による暗号化処理、鍵２による暗号化処理、さらに鍵３による暗号化処理の順に処理を行い３回とも暗号化処理を行う。鍵は、Ｋ１、Ｋ２、Ｋ３の順に３種類の鍵を用いる。このように複数の処理を連続させる構成とすることで、シングルＤＥＳに比較してセキュリティ強度を向上させている。しかしながら、このトリプルＤＥＳ（Triple ＤＥＳ）構成は、処理時間がシングルＤＥＳのおよそ３倍かかるという欠

点を有する。

【０１１０】

図８および図９で説明したトリプルＤＥＳ構成を改良したＭＡＣ値生成構成例を図１０に示す。図１０においては、署名対象となるメッセージ列の初めから途中までの各メッセージに対する暗号化処理は全てシングルＤＥＳによる処理とし、最後のメッセージに対する暗号化処理のみを図９（ａ）に示すトリプルＤＥＳ（Triple ＤＥＳ）構成としたものである。

【０１１１】

図１０に示すこのような構成とすることで、メッセージのＭＡＣ値の生成処理時間は、シングルＤＥＳによるＭＡＣ値生成処理に要する時間とほぼ同程度に短縮され、かつセキュリティはシングルＤＥＳによるＭＡＣ値よりも高めることが可能となる。なお、最終メッセージに対するトリプルＤＥＳ構成は、図９（ｂ）の構成とすることも可能である。

【０１１２】

（３－２）公開鍵暗号方式による電子署名

以上は、暗号化方式として共通鍵暗号化方式を適用した場合の電子署名データの生成方法であるが、次に、暗号化方式として公開鍵暗号方式を用いた電子署名の生成方法を図１１を用いて説明する。図１１に示す処理は、ＥＣ－ＤＳＡ（（Elliptic Curve Digital Signature Algorithm）、IEEE P1363/D3）を用いた電子署名データの生成処理フローである。なお、ここでは公開鍵暗号として楕円曲線暗号（Elliptic Curve Cryptography（以下、ECCと呼ぶ））を用いた例を説明する。なお、本発明のデータ処理装置においては、楕円曲線暗号以外にも、同様の公開鍵暗号方式における、例えばＲＳＡ暗号（（Rivest、Shamir、Adleman）など（ANSI X9.31））を用いることも可能である。

【０１１３】

図１１の各ステップについて説明する。ステップＳ１において、pを標数、a、bを楕円曲線の係数（楕円曲線：$y^2=x^3+ax+b$）、Gを楕円曲線上のベースポイント、rをGの位数、Ｋｓを秘密鍵（０＜Ｋｓ＜ｒ）とする。ステップＳ２おいて、メッセージＭのハッシュ値を計算し、f=Hash(M)とする。

【０１１４】

ここで、ハッシュ関数を用いてハッシュ値を求める方法を説明する。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、ＭＤ４、ＭＤ５、ＳＨＡ－１などが用いられる場合もあるし、図７他で説明したと同様のＤＥＳ－ＣＢＣが用いられる場合もある。この場合は、最終出力値となるＭＡＣ（チェック値：ＩＣＶに相当する）がハッシュ値となる。

【０１１５】

続けて、ステップＳ３で、乱数ｕ（０＜ｕ＜ｒ）を生成し、ステップＳ４でベースポイントをｕ倍した座標Ｖ（Ｘｖ，Ｙｖ）を計算する。なお、楕円曲線上の加算、２倍算は次のように定義されている。

【０１１６】

【数１】

$P=(Xa, Ya), Q=(Xb, Yb), R=(Xc, Yc)=P+Q$とすると、

$P \neq Q$の時（加算）、

$Xc=\lambda^2-Xa-Xb$

$Yc=\lambda\times(Xa-Xc)-Ya$

$\lambda=(Yb-Ya)/(Xb-Xa)$

$P=Q$の時（2倍算）、

$Xc=\lambda^2-2Xa$

$Yc=\lambda\times(Xa-Xc)-Ya$

$\lambda=(3(Xa)^2+a)/(2Ya)$

【０１１７】

これらを用いて点Ｇのｕ倍を計算する（速度は遅いが、最もわかりやすい演算方法として次のように行う。Ｇ、２×Ｇ、４×Ｇ・・を計算し、uを2進数展開して1が立っているところに対応する$2^i\times G$（Ｇをｉ回２倍算した値）を加算する（ｉはｕのＬＳＢから数えた時のビット位置））。

【０１１８】

ステップＳ５で、ｃ＝Ｘｖｍｏｄ　ｒを計算し、ステップＳ６でこの値が０になるかどうか判定し、０でなければステップＳ７でｄ＝［（ｆ＋ｃＫｓ）／ｕ］ｍｏｄ　ｒを計算し、ステップＳ８でｄが０であるかどうか判定し、ｄが０でなければ、ステップＳ９でｃおよびｄを電子署名データとして出力する。仮に、ｒを１６０ビット長の長さであると仮定すると、電子署名データは３２０ビット長となる。

【０１１９】

ステップＳ６において、ｃが０であった場合、ステップＳ３に戻って新たな乱数を生成し直す。同様に、ステップＳ８でｄが０であった場合も、ステップＳ３に戻って乱数を生成し直す。

【０１２０】

（３－３）公開鍵暗号方式による電子署名の検証

次に、公開鍵暗号方式を用いた電子署名の検証方法を、図１２を用いて説明する。ステップＳ１１で、Ｍをメッセージ、ｐを標数、ａ、ｂを楕円曲線の係数（楕円曲線：$y^2=x^3+ax+b$）、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、ＧおよびＫｓ×Ｇを公開鍵（０＜Ｋｓ＜ｒ）とする。ステップＳ１２で電子署名データｃおよびｄが０＜ｃ＜ｒ、０＜ｄ＜ｒを満たすか検証する。これを満たしていた場合、ステップＳ１３で、メッセージＭのハッシュ値を計算し、ｆ＝Ｈａｓｈ（Ｍ）とする。次に、ステップＳ１４で$h=1/d \bmod r$を計算し、ステップＳ１５でｈ１＝ｆｈ　ｍｏｄ　ｒ、ｈ２＝ｃｈ　ｍｏｄ　ｒを計算する。

【０１２１】

ステップＳ１６において、既に計算したｈ１およびｈ２を用い、点Ｐ＝（Ｘｐ，Ｙｐ）＝ｈ１×Ｇ＋ｈ２・Ｋｓ×Ｇを計算する。電子署名検証者は、公開鍵ＧおよびＫｓ×Ｇを知っているので、図１１のステップＳ４と同様に楕円曲線上の点のスカラー倍の計算ができる。そして、ステップＳ１７で点Ｐが無限遠点かどうか判定し、無限遠点でなければステップＳ１８に進む（実際には、無限遠点の判定はステップＳ１６でできてしまう。つまり、Ｐ＝（Ｘ，Ｙ）、Ｑ＝（Ｘ，－Ｙ）の加算を行うと、λが計算できず、Ｐ＋Ｑが無限遠点であることが判明して

いる）。ステップＳ１８でＸｐ ｍｏｄ ｒを計算し、電子署名データｃと比較する。最後に、この値が一致していた場合、ステップＳ１９に進み、電子署名が正しいと判定する。

【０１２２】

電子署名が正しいと判定された場合、データは改竄されておらず、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したことがわかる。

【０１２３】

ステップＳ１２において、電子署名データｃまたはｄが、０＜ｃ＜ｒ、０＜ｄ＜ｒを満たさなかった場合、ステップＳ２０に進む。また、ステップＳ１７において、点Pが無限遠点であった場合もステップＳ２０に進む。さらにまた、ステップＳ１８において、Ｘｐ ｍｏｄ ｒの値が、電子署名データｃと一致していなかった場合にもステップＳ２０に進む。

【０１２４】

ステップＳ２０において、電子署名が正しくないと判定された場合、データは改竄されているか、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したのではないことがわかる。

【０１２５】

（３－４）共通鍵暗号方式による相互認証

次に、共通鍵暗号方式を用いた相互認証方法を、図１３を用いて説明する。図１３において、共通鍵暗号方式としてＤＥＳを用いているが、前述のように同様な共通鍵暗号方式であればいずれでもよい。図１３において、まず、Ｂが６４ビットの乱数Ｒｂを生成し、Ｒｂおよび自己のIDであるＩＤ（ｂ）をＡに送信する。これを受信したＡは、新たに64ビットの乱数Ｒａを生成し、Ｒａ、Ｒｂ、ＩＤ（ｂ）の順に、ＤＥＳのＣＢＣモードで鍵Ｋａｂを用いてデータを暗号化し、Ｂに返送する。図７に示すＤＥＳのＣＢＣモード処理構成によれば、ＲａがＭ１、ＲｂがＭ２、ＩＤ（ｂ）がＭ３に相当し、初期値：ＩＶ＝０としたときの出力Ｅ１、Ｅ２、Ｅ３が暗号文となる。

【０１２６】

これを受信したＢは、受信データを鍵Ｋａｂで復号化する。受信データの復号

化方法は、まず、暗号文Ｅ１を鍵Ｋａｂで復号化し、乱数Ｒａを得る。次に、暗号文Ｅ２を鍵Ｋａｂで復号化し、その結果とＥ１を排他的論理和し、Ｒｂを得る。最後に、暗号文Ｅ３を鍵Ｋａｂで復号化し、その結果とＥ２を排他的論理和し、ＩＤ(ｂ)を得る。こうして得られたＲａ、Ｒｂ、ＩＤ(ｂ)の内、ＲｂおよびＩＤ(ｂ)が、Ｂが送信したものと一致するか検証する。この検証に通った場合、ＢはＡを正当なものとして認証する。

【０１２７】

次にＢは、認証後に使用するセッション鍵（Session Key（以下、Ｋｓｅｓとする））を生成する（生成方法は、乱数を用いる）。そして、Ｒｂ、Ｒａ、Ｋｓｅｓの順に、ＤＥＳのＣＢＣモードで鍵Ｋａｂを用いて暗号化し、Ａに返送する。

【０１２８】

これを受信したＡは、受信データを鍵Ｋａｂで復号化する。受信データの復号化方法は、Ｂの復号化処理と同様であるので、ここでは詳細を省略する。こうして得られたＲｂ、Ｒａ、Ｋｓｅｓの内、ＲｂおよびＲａが、Ａが送信したものと一致するか検証する。この検証に通った場合、ＡはＢを正当なものとして認証する。互いに相手を認証した後には、セッション鍵Ｋｓｅｓは、認証後の秘密通信のための共通鍵として利用される。

【０１２９】

なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【０１３０】

（３－５）公開鍵証明書

次に、公開鍵証明書について図１４を用いて説明する。公開鍵証明書は、公開鍵暗号方式における認証局（ＣＡ：Certificate Authority）が発行する証明書であり、ユーザが自己のＩＤ、公開鍵等を認証局に提出することにより、認証局側が認証局のＩＤや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

【０１３１】

図１４に示す公開鍵証明書は、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前（ユーザＩＤ）、証明書利用者の公開鍵並びに電子署名を含む。

【０１３２】

電子署名は、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前並びに証明書利用者の公開鍵全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して認証局の秘密鍵を用いて生成したデータである。この電子署名の生成には、例えば図１１で説明した処理フローが適用される。

【０１３３】

認証局は、図１４に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布（これをリボケーション：Revocationと呼ぶ）を行う。また、必要に応じて公開鍵・秘密鍵の生成も行う。

【０１３４】

一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。なお、電子署名の検証方法については、図１２で説明したのでその詳細は省略する。

【０１３５】

（３－６）公開鍵暗号方式による相互認証

次に、公開鍵暗号方式である１６０ビット長の楕円曲線暗号を用いた相互認証方法を、図１５を用いて説明する。図１５において、公開鍵暗号方式としてＥＣＣを用いているが、前述のように同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも１６０ビットでなくてもよい。図１５において、まずＢが、

６４ビットの乱数Ｒｂを生成し、Aに送信する。これを受信したＡは、新たに６４ビットの乱数Ｒａおよび標数ｐより小さい乱数Ａｋを生成する。そして、ベースポイントＧをＡｋ倍した点Ａｖ＝Ａｋ×Ｇを求め、Ｒａ、Ｒｂ、Ａｖ（X座標とY座標）に対する電子署名Ａ．Ｓｉｇを生成し、Ａの公開鍵証明書とともにＢに返送する。ここで、ＲａおよびＲｂはそれぞれ６４ビット、ＡｖのＸ座標とＹ座標がそれぞれ１６０ビットであるので、合計４４８ビットに対する電子署名を生成する。電子署名の生成方法は図１１で説明したので、その詳細は省略する。また、公開鍵証明書も図１４で説明したので、その詳細は省略する。

【０１３６】

Ａの公開鍵証明書、Ｒａ、Ｒｂ、Ａｖ、電子署名Ａ．Ｓｉｇを受信したＢは、Ａが送信してきたＲｂが、Ｂが生成したものと一致するか検証する。その結果、一致していた場合には、Ａの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Ａの公開鍵を取り出す。公開鍵証明書の検証については、図１４を用いて説明したので、その詳細は省略する。そして、取り出したＡの公開鍵を用い電子署名Ａ．Ｓｉｇを検証する。電子署名の検証方法は図１２で説明したので、その詳細は省略する。電子署名の検証に成功した後、ＢはＡを正当なものとして認証する。

【０１３７】

次に、Ｂは、標数ｐより小さい乱数Ｂｋを生成する。そして、ベースポイントＧをＢｋ倍した点Ｂｖ＝Ｂｋ×Ｇを求め、Ｒｂ、Ｒａ、Ｂｖ（Ｘ座標とＹ座標）に対する電子署名Ｂ．Ｓｉｇを生成し、Ｂの公開鍵証明書とともにＡに返送する。

【０１３８】

Ｂの公開鍵証明書、Ｒｂ、Ｒａ、Ａｖ、電子署名Ｂ．Ｓｉｇを受信したＡは、Ｂが送信してきたＲａが、Ａが生成したものと一致するか検証する。その結果、一致していた場合には、Ｂの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Ｂの公開鍵を取り出す。そして、取り出したＢの公開鍵を用い電子署名Ｂ．Ｓｉｇを検証する。電子署名の検証に成功した後、ＡはＢを正当なものとして認証する。

【０１３９】

両者が認証に成功した場合には、ＢはＢｋ×Ａｖ（Ｂｋは乱数だが、Ａｖは楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要）を計算し、ＡはＡｋ×Ｂｖを計算し、これら点のＸ座標の下位６４ビットをセッション鍵として以降の通信に使用する（共通鍵暗号を６４ビット鍵長の共通鍵暗号とした場合）。もちろん、Ｙ座標からセッション鍵を生成してもよいし、下位６４ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッション鍵で暗号化されるだけでなく、電子署名も付されることがある。

【０１４０】

電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【０１４１】

（３－７）楕円曲線暗号を用いた暗号化処理

次に、楕円曲線暗号を用いた暗号化について、図１６を用いて説明する。ステップＳ２１において、Ｍｘ、Ｍｙをメッセージ、ｐを標数、ａ、ｂを楕円曲線の係数（楕円曲線：$y^2=x^3+ax+b$）、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、ＧおよびＫｓ×Ｇを公開鍵（０＜Ｋｓ＜ｒ）とする。ステップＳ２２で乱数ｕを０＜ｕ＜ｒになるように生成し、ステップＳ２３で公開鍵Ｋｓ×Ｇをｕ倍した座標Ｖを計算する。なお、楕円曲線上のスカラー倍は図１１のステップＳ４で説明したので、詳細は省略する。ステップＳ２４で、ＶのＸ座標をＭｘ倍してｐで剰余を求めＸ０とし、ステップＳ２５でＶのＹ座標をＭｙ倍してｐで剰余を求めＹ０とする。なお、メッセージの長さがｐのビット数より少ない場合、Ｍｙは乱数を使い、復号化部ではＭｙを破棄するようにする。ステップＳ２６において、ｕ×Ｇを計算し、ステップＳ２７で暗号文ｕ×Ｇ、（Ｘ０、Ｙ０）を得る。

【０１４２】

（３－８）楕円曲線暗号を用いた復号化処理

次に、楕円曲線暗号を用いた復号化について、図１７を用いて説明する。ステップＳ３１において、ｕ×Ｇ、（Ｘ０、Ｙ０）を暗号文データ、ｐを標数、ａ、ｂを楕円曲線の係数（楕円曲線：$y^2=x^3+ax+b$）、Ｇを楕円曲線上のベース

ポイント、rをGの位数、Ｋｓを秘密鍵（０＜Ｋｓ＜ｒ）とする。ステップｓ３２において、暗号データｕ×Ｇを秘密鍵Ｋｓ倍し、座標Ｖ（Ｘｖ，Ｙｖ）を求める。ステップＳ３３では、暗号データの内、（Ｘ０、Ｙ０）のX座標を取り出し、Ｘ１＝Ｘ０／Ｘｖ mod ｐを計算し、ステップＳ３４においては、Ｙ座標を取り出し、Ｙ１＝Ｙ０／Ｙｖ mod ｐを計算する。そして、ステップＳ３５でＸ１をＭｘとし、Ｙ１をＭｙとしてメッセージを取り出す。この時、Ｍｙをメッセージにしていなかった場合、Ｙ１は破棄する。

【０１４３】

このように、秘密鍵をＫｓ、公開鍵をＧ、Ｋｓ×Ｇとすることで、暗号化に使用する鍵と復号化に使用する鍵を、異なる鍵とすることができる。

【０１４４】

また、公開鍵暗号の他の例としてはＲＳＡ暗号が知られているが、詳しい説明は省略する（PKCS #1 Version2に詳細が記述されている）。

【０１４５】

（３－９）乱数生成処理

次に、乱数の生成方法について説明する。乱数の生成方法としては、熱雑音を増幅し、そのＡ／Ｄ出力から生成する真性乱数生成法や、Ｍ系列等の線形回路を複数組み合わせて生成する疑似乱数生成法等が知られている。また、ＤＥＳ等の共通鍵暗号を用いて生成する方法も知られている。本例では、ＤＥＳを用いた疑似乱数生成方法について説明する（ANSI X9.17ベース）。

【０１４６】

まず、時間等のデータから得られた６４ビット（これ以下のビット数の場合、上位ビットを0とする）の値をＤ、Ｔｒｉｐｌｅ－ＤＥＳに使われる鍵情報をＫｒ、乱数発生用の種（Ｓｅｅｄ）をＳとする。このとき、乱数Ｒは以下のように計算される。

【０１４７】

【数２】

$$I=\text{Triple-DES}(Kr, D) \cdots\cdots\cdots (2-1)$$
$$R=\text{Triple-DES}(Kr, S \hat{} I) \cdots\cdots\cdots (2-2)$$
$$S=\text{Triple-DES}(Kr, R \hat{} I) \cdots\cdots\cdots (2-3)$$

【０１４８】

ここで、Ｔｒｉｐｌｅ－ＤＥＳ（）は、第１引数を暗号鍵情報として、第２引数の値をＴｒｉｐｌｅ－ＤＥＳで暗号化する関数とし、演算＾は６４ビット単位の排他的論理和、最終的にでてきた値Ｓは、新規のＳｅｅｄ（種）として更新されていくものとする。

【０１４９】

以下、連続して乱数を生成する場合には、（２－２）式、（２－３）式を繰り返すものとする。

【０１５０】

以上、本発明のデータ処理装置において適用可能な暗号処理に関する各種処理態様について説明した。次に、本発明のデータ処理装置において実行される具体的な処理について、詳細に説明する。

【０１５１】

（４）記録再生器の格納データ構成

図１８は、図３で示す記録再生器３００での記録再生器暗号処理部３０２に構成された内部メモリ３０７のデータ保持内容を説明する図である。

【０１５２】

図１８に示すように、内部メモリ３０７には、以下の鍵、データが格納されている。

ＭＫａｋｅ：記録再生器３００と記録デバイス４００（図３参照）との間で実行される相互認証処理に必要な認証鍵（Authentication and Key Exchange Key（以下、Ｋａｋｅとする））を生成するための記録デバイス認証鍵用マスター鍵。

ＩＶａｋｅ：記録デバイス認証鍵用初期値。

ＭＫｄｉｓ：配送鍵Ｋｄｉｓを生成するための配送鍵用マスター鍵。

ＩＶｄｉｓ：配送鍵生成用初期値。

Ｋｉｃｖａ：チェック値ＩＣＶａを生成するための鍵であるチェック値Ａ生成鍵。

Ｋｉｃｖｂ：チェック値ＩＣＶｂを生成するための鍵であるチェック値Ｂ生成鍵。

Ｋｉｃｖｃ：各コンテンツブロックのチェック値ＩＣＶｉ（ｉ＝１～Ｎ）を生成するための鍵であるコンテンツチェック値生成鍵。

Ｋｉｃｖｔ：総チェック値ＩＣＶｔを生成するための鍵である総チェック値生成鍵。

Ｋｓｙｓ：配信システムに共通の署名またはＩＣＶをつけるために使用するシステム署名鍵。

Ｋｄｅｖ：記録再生器毎に異なり、記録再生器が署名またはＩＣＶをつけるために使用する記録再生器固有の記録再生器署名鍵。

ＩＶｍｅｍ：初期値、相互認証処理等の際の暗号処理に用いられる初期値。記録デバイスと共通。

これらの鍵、データが記録再生器暗号処理部３０２に構成された内部メモリ３０７に格納されている。

【０１５３】

（５）記録デバイスの格納データ構成

図１９は、記録デバイス上でのデータ保持状況を示す図である。図１９において、内部メモリ４０５は、複数のブロック（本例ではＮブロック）に分割されており、それぞれのブロック中に、以下の鍵、データが格納されている。

ＩＤｍｅｍ：記録デバイス識別情報、記録デバイス固有の識別情報。

Ｋａｋｅ：認証鍵、記録再生器３００との相互認証時に用いる認証鍵。

ＩＶｍｅｍ：初期値、相互認証処理等の際の暗号処理に用いられる初期値。

Ｋｓｔｒ：保存鍵、ブロック情報鍵他のコンテンツデータの暗号鍵。

Ｋｒ：乱数生成鍵、

Ｓ：種

これらのデータを個別のブロックに各々保持している。外部メモリ４０２は複

数（本例ではM個）のコンテンツデータを保持しており、それぞれ図４で説明したデータを、例えば図２６、または図２７のように保持している。図２６、図２７の構成の差異については後段で説明する。

【０１５４】

（６）記録再生器、記録デバイス間における相互認証処理

（６－１）相互認証処理の概要

図２０は、記録再生器３００と記録デバイス４００との認証手順を示す流れ図である。ステップＳ４１において、利用者が記録デバイス４００を記録再生器３００に挿入する。ただし非接触で通信できる記録デバイスを使用する場合には、挿入する必要はない。

【０１５５】

記録再生器３００に記録デバイス４００をセットすると、図３に示す記録再生器３００内の記録デバイス検知手段（図示せず）が、制御部３０１に記録デバイス４００の装着を通知する。次に、ステップＳ４２において、記録再生器３００の制御部３０１は、記録デバイスコントローラ３０３を介して記録デバイス４００に初期化命令を送信する。これを受信した記録デバイス４００は、記録デバイス暗号処理部４０１の制御部４０３において、通信部４０４を介して命令を受信し、認証完了フラグがセットされていればクリアする。すなわち未認証状態に設定する。

【０１５６】

次に、ステップＳ４３において、記録再生器３００の制御部３０１は、記録再生器暗号処理部３０２に初期化命令を送信する。このとき、記録デバイス挿入口番号も併せて送信する。記録デバイス挿入口番号を送信することにより、記録再生器３００に複数の記録デバイスが接続された場合であっても同時に複数の記録デバイス４００との認証処理、およびデータ送受信が可能となる。

【０１５７】

初期化命令を受信した記録再生器３００の記録再生器暗号処理部３０２は、記録再生器暗号処理部３０２の制御部３０６において、記録デバイス挿入口番号に対応する認証完了フラグがセットされていればクリアする。すなわち未認証状態

に設定する。

【０１５８】

次に、ステップＳ４４において、記録再生器３００の制御部３０１は、記録デバイス４００の記録デバイス暗号処理部４０１が使う鍵ブロック番号を指定する。なお、鍵ブロック番号の詳細に関しては後述する。ステップＳ４５において、記録再生器３００の制御部３０１は、記録デバイス４００の内部メモリ４０５の指定された鍵ブロックに格納された記録デバイス識別情報ＩＤｍｅｍを読み出す。ステップＳ４６において、記録再生器３００の制御部３０１は、記録再生器暗号処理部３０２に記録デバイス識別情報ＩＤｍｅｍを送信し、記録デバイス識別情報ＩＤｍｅｍに基づく認証鍵Ｋａｋｅを生成させる。認証鍵Ｋａｋｅの生成方法としては、例えば次のように生成する。

【０１５９】

【数３】

$$Kake=DES(MKake,\ IDmem \hat{}\ IVake)$$

【０１６０】

ここで、ＭＫａｋｅは、記録再生器３００と記録デバイス４００（図３参照）との間で実行される相互認証処理に必要な認証鍵Ｋａｋｅを生成するための記録デバイス認証鍵用マスター鍵であり、これは、前述したように記録再生器３００の内部メモリ３０７に格納されている鍵である。またＩＤｍｅｍは、記録デバイス４００に固有の記録デバイス識別情報である。さらにＩＶａｋｅは、記録デバイス認証鍵用初期値である。また、上記式において、ＤＥＳ（）は、第１引数を暗号鍵として、第２引数の値をＤＥＳで暗号化する関数であり、演算＾は６４ビット単位の排他的論理和を示す。

【０１６１】

例えば図７、図８に示すＤＥＳ構成を適用する場合には、図７，８に示されるメッセージＭを記録デバイス識別情報：ＩＤｍｅｍとし、鍵Ｋ１をデバイス認証鍵用マスター鍵：ＭＫａｋｅとし、初期値ＩＶを：ＩＶａｋｅとして得られる出力が認証鍵Ｋａｋｅとなる。

【０１６２】

次に、ステップＳ４７で相互認証およびセッション鍵Ｋｓｅｓの生成処理を行う。相互認証は、記録再生器暗号処理部３０２の暗号／復号化部３０８と記録デバイス暗号処理部４０１の暗号／復号化部４０６の間で行われ、その仲介を記録再生器３００の制御部３０１が行っている。

【０１６３】

相互認証処理は、例えば前述の図１３で説明した処理にしたがって実行することができる。図１３に示す構成において、Ａ、Ｂがそれぞれ記録再生器３００と記録デバイス４００に対応する。まず、記録再生器３００の記録再生器暗号処理部３０２が乱数Ｒｂを生成し、乱数Ｒｂおよび自己のＩＤである記録再生器識別情報ＩＤｄｅｖを記録デバイス４００の記録デバイス暗号処理部４０１に送信する。なお、記録再生器識別情報ＩＤｄｅｖは、記録再生器３００内に構成された記憶部に記憶された再生器固有の識別子である。記録再生器暗号処理部３０２の内部メモリ中に記録再生器識別情報ＩＤｄｅｖを記録する構成としてもよい。

【０１６４】

乱数Ｒｂおよび記録再生器識別情報ＩＤｄｅｖを受信した記録デバイス４００の記録デバイス暗号処理部４０１は、新たに６４ビットの乱数Ｒａを生成し、Ｒａ、Ｒｂ、と記録再生器識別情報ＩＤｄｅｖの順に、ＤＥＳのＣＢＣモードで認証鍵Ｋａｋｅを用いてデータを暗号化し、記録再生器３００の記録再生器暗号処理部３０２に返送する。例えば、図７に示すＤＥＳのＣＢＣモード処理構成によれば、ＲａがＭ１、ＲｂがＭ２、ＩＤｄｅｖがＭ３に相当し、初期値：ＩＶ＝ＩＶｍｅｍとしたときの出力Ｅ１、Ｅ２、Ｅ３が暗号文となる。

【０１６５】

暗号文Ｅ１、Ｅ２、Ｅ３を受信した記録再生器３００の記録再生器暗号処理部３０２は、受信データを認証鍵Ｋａｋｅで復号化する。受信データの復号化方法は、まず、暗号文Ｅ１を認証鍵Ｋａｋｅで復号化し、その結果とＩＶｍｅｍとを排他的論理和し、乱数Ｒａを得る。次に、暗号文Ｅ２を認証鍵Ｋａｋｅで復号化し、その結果とＥ１を排他的論理和し、Ｒｂを得る。最後に、暗号文Ｅ３を認証鍵Ｋａｋｅで復号化し、その結果とＥ２を排他的論理和し、記録再生器識別情報

ＩＤｄｅｖを得る。こうして得られたＲａ、Ｒｂ、記録再生器識別情報ＩＤｄｅｖの内、ＲｂおよびＩＤｄｅｖが、記録再生器３００が送信したものと一致するか検証する。この検証に通った場合、記録再生器３００の記録再生器暗号処理部３０２は記録デバイス４００を正当なものとして認証する。

【０１６６】

次に、記録再生器３００の記録再生器暗号処理部３０２は、認証後に使用するセッション鍵（Session Key（以下、Ｋｓｅｓとする））を生成する（生成方法は、乱数を用いる）。そして、Ｒｂ、Ｒａ、Ｋｓｅｓの順に、ＤＥＳのＣＢＣモードで鍵Ｋａｋｅ、初期値ＩＶｍｅｍを用いて暗号化し、記録デバイス４００の記録デバイス暗号処理部４０１に返送する。

【０１６７】

これを受信した記録デバイス４００の記録デバイス暗号処理部４０１は、受信データを鍵Ｋａｋｅで復号化する。受信データの復号化方法は、記録再生器３００の記録再生器暗号処理部３０２における復号化処理と同様であるので、ここでは詳細を省略する。こうして得られたＲｂ、Ｒａ、Ｋｓｅｓの内、ＲｂおよびＲａが、記録デバイス４００が送信したものと一致するか検証する。この検証に通った場合、記録デバイス４００の記録デバイス暗号処理部４０１は記録再生器３００を正当なものとして認証する。互いに相手を認証した後には、セッション鍵Ｋｓｅｓは、認証後の秘密通信のための共通鍵として利用される。

【０１６８】

なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【０１６９】

相互認証に成功した場合には、ステップＳ４８からステップＳ４９に進み、セッション鍵Ｋｓｅｓを記録再生器３００の記録再生器暗号処理部３０２で保持するとともに、相互認証が終了したことを示す認証完了フラグをセットする。また、相互認証に失敗した場合には、ステップＳ５０に進み、認証処理過程で生成されたセッション鍵Ｋｓｅｓを破棄するとともに、認証完了フラグをクリアする。なお、すでにクリアされている場合には必ずしもクリア処理は必要ではない。

【０１７０】

なお、記録デバイス４００が記録デバイス挿入口から取り除かれた場合には、記録再生器３００内の記録デバイス検知手段が、記録再生器３００の制御部３０１に記録デバイス４００が取り除かれたことを通知し、これを受けた記録再生器３００の制御部３０１は、記録再生器３００の記録再生器暗号処理部３０２に対し記録デバイス挿入口番号に対応する認証完了フラグをクリアするように命令し、これを受けた記録再生器３００の記録再生器暗号処理部３０２は、記録デバイス挿入口番号に対応する認証完了フラグをクリアする。

【０１７１】

なお、ここでは相互認証処理を図１３に示す手続きにしたがって実行する例について説明したが、上述した認証処理例に限らず、例えば先に説明した図１５の相互認証手続きに従った処理を実行してもよい。また、図１３に示す手続きにおいて、図１３のＡを記録再生器３００とし、Ｂを記録デバイス４００とし、Ｂ：記録デバイス４００がＡ：記録再生器３００に最初に送付するＩＤを記録デバイス中の鍵ブロック中の記録デバイス識別情報として相互認証処理を行なってもよい。本発明において実行される認証処理手続きは、様々な処理が適用可能であり、上述の認証処理に限定されるものではない。

【０１７２】

（６－２）相互認証時の鍵ブロックの切り替え

本発明のデータ処理装置における相互認証処理における１つの特徴は、記録デバイス４００側に複数の鍵ブロック（ｅｘ．Ｎ個の鍵ブロック）を構成して、記録再生器３００が１つの鍵ブロックを指定（図２０の処理フローにおけるステップＳ４４）して認証処理を実行する点である。先に図１９において説明したように、記録デバイス４００の暗号処理部４０１に構成された内部メモリ４０５には複数の鍵ブロックが形成されており、それぞれが異なる鍵データ、ＩＤ情報等各種データを格納している。図２０で説明した記録再生器３００と記録デバイス４００間で実行される相互認証処理は、図１９の記録デバイス４００の複数の鍵ブロックの１つの鍵ブロックに対して実行される。

【０１７３】

従来、記憶媒体とその再生機器間における相互認証処理を実行する構成では、相互認証に用いる鍵：認証鍵は共通なものが使用されるのが一般的であった。従って、例えば製品仕向け先（国別）ごと、あるいは製品ごとに認証鍵を変更しようとすると、記録再生器側と、記録デバイス側の認証処理に必要となる鍵データを双方の機器において変更することが必要となる。従って例えば新たに発売された記録再生器に格納された認証処理に必要となる鍵データは、先に販売された記録デバイスに格納された認証処理に必要となる鍵データに対応せず、新たな記録再生器は、古いバージョンの記録デバイスへのアクセスができなくなってしまう事態が発生する。逆に新しいバージョンの記録デバイスと古いバージョンの記録再生器との関係においても同様の事態が発生する。

【０１７４】

本発明のデータ処理装置においては、図１９に示すように予め記録デバイス４００に複数の異なる鍵セットとしての鍵ブロックが格納されている。記録再生器は例えば製品仕向け先（国別）ごと、あるいは製品、機種、バージョン、アプリケーションごとに、認証処理に適用すべき鍵ブロック、すなわち指定鍵ブロックが設定される。この設定情報は、記録再生器のメモリ部、例えば、図３における内部メモリ３０７、あるいは、記録再生器３００の有するその他の記憶素子内に格納され、認証処理時に図３の制御部３０１によってアクセスされ設定情報にしたがった鍵ブロック指定が行われる。

【０１７５】

記録再生器３００の内部メモリ３０７の記録デバイス認証鍵用マスター鍵ＭＫａｋｅは、それぞれの指定鍵ブロックの設定に従って設定された認証鍵用マスター鍵であり、指定鍵ブロックにのみ対応可能となっており、指定鍵ブロック以外の鍵ブロックとの相互認証は成立しない構成となっている。

【０１７６】

図１９から理解されるように、記録デバイス４００の内部メモリ４０５には１～ＮのＮ個の鍵ブロックが設定され、各鍵ブロック毎に記録デバイス識別情報、認証鍵、初期値、保存鍵、乱数生成鍵、種が格納され、少なくとも認証用のかぎデータがブロック毎に異なるデータとして格納されている。

【０１７７】

このように、記録デバイス４００の鍵ブロックの鍵データ構成は、ブロック毎に異なっている。従って、例えば、ある記録再生機器Ａが内部メモリに格納された記録デバイス認証鍵用マスター鍵ＭＫａｋｅを用いて認証処理を行ない得る鍵ブロックは鍵ブロックＮｏ．１であり、また別の仕様の記録再生器Ｂが認証可能な鍵ブロックは別の鍵ブロック、例えば鍵ブロックＮｏ．２のように設定することが可能となる。

【０１７８】

後段でさらに詳細に説明するが、コンテンツを記録デバイス４００の外部メモリ４０２に格納する際、各鍵ブロックに格納された保存鍵Ｋｓｔｒを用いて暗号化処理がなされ、格納されることになる。より、具体的には、コンテンツブロックを暗号化するコンテンツ鍵を保存鍵で暗号化処理する。

【０１７９】

図１９に示すように保存鍵は、各ブロック毎に異なる鍵として構成されている。従って、異なる鍵ブロックを指定するように設定された２つの異なる設定の記録再生器間においては、ある１つの記録デバイスのメモリに格納されたコンテンツを両者で共通に利用することは防止される。すなわち、異なる設定のなされた記録再生器は、それぞれの設定に合致する記録デバイスに格納されたコンテンツのみが利用できる。

【０１８０】

なお、各鍵ブロックについて共通化可能なデータは共通化することも可能であり、例えば認証用の鍵データ、保存鍵データのみを異なるように構成してもよい。

【０１８１】

このような記録デバイスに複数の異なる鍵データからなる鍵ブロックを構成する具体例としては、例えば記録再生器３００の機種別（据え置き型、携帯型等）で指定すべき鍵ブロック番号を異なるように設定したり、あるいは、アプリケーション毎に指定鍵ブロックを異なるように設定する例がある。さらに、例えば日本で販売する記録再生器については指定鍵ブロックをＮｏ．１とし、米国で販売

する記録再生器は指定鍵ブロックをＮｏ．２とするように地域ごとに異なる鍵ブロック設定を行なう構成とすることも可能である。このような構成とすることで、それぞれの異なる販売地域で使用され、記録デバイスに異なる保存鍵で格納されたコンテンツは、たとえメモリカードのような記録デバイスが米国から日本、あるいは日本から米国へ転送されてきても、異なる鍵設定のなされた記録再生器で利用することは不可能であるので、メモリに格納したコンテンツの不正、無秩序な流通を防止できる。具体的には、異なる保存鍵Ｋｓｔｒで暗号化されているコンテンツ鍵Ｋｃｏｎが２国間で相互に利用可能となる状態を排除することができる。

【０１８２】

さらに、図１９に示す記録デバイス４００の内部メモリ４０５の鍵ブロック１～Ｎまでの少なくとも１つの鍵ブロック、例えばＮｏ．Ｎの鍵ブロックをいずれの記録再生器３００においても共通に利用可能な鍵ブロックとして構成してもよい。

【０１８３】

例えば、全ての機器に鍵ブロックＮｏ．Ｎとの認証可能な記録デバイス認証鍵用マスター鍵ＭＫａｋｅを格納することで、記録再生器３００の機種別、アプリケーション毎、仕向け国毎等に無関係に流通可能なコンテンツとして扱うことができる。例えば、鍵ブロックＮｏ．Ｎに格納された保存鍵でメモリカードに格納された暗号化コンテンツは、すべての機器において利用可能なコンテンツとなる。例えば、音楽データ等を共通に利用可能な鍵ブロックの保存鍵で暗号化してメモリカードに記憶し、このメモリカードを、やはり共通の記録デバイス認証鍵用マスター鍵ＭＫａｋｅを格納した例えば携帯型の音声再生機器等にセットすることで、メモリカードからのデータの復号再生処理を可能とすることができる。

【０１８４】

本発明のデータ処理装置における複数の鍵ブロックを有する記録デバイスの利用例を図２１に示す。記録再生器２１０１は日本向け製品の記録再生器であり、記録デバイスの鍵ブロックのＮｏ．１，４との間での認証処理が成立するマスター鍵を持っている。記録再生器２１０２はＵＳ向け製品の記録再生器であり、記

録デバイスの鍵ブロックのＮｏ．２，４との間での認証処理が成立するマスター鍵を持っている。記録再生器２１０３はＥＵ向け製品の記録再生器であり、記録デバイスの鍵ブロックのＮｏ．３，４との間での認証処理が成立するマスター鍵を持っている。

【０１８５】

例えば記録再生器２１０１は、記録デバイスＡ，２１０４の鍵ブロック１または鍵ブロック４との間で認証が成立し、それぞれの鍵ブロックに格納された保存鍵を介した暗号処理を施したコンテンツが外部メモリに格納される。記録再生器２１０２は、記録デバイスＢ，２１０５の鍵ブロック２または鍵ブロック４との間で認証が成立し、それぞれの鍵ブロックに格納された保存鍵を介した暗号処理を施したコンテンツが外部メモリに格納される。記録再生器２１０３は、記録デバイスＣ，２１０６の鍵ブロック３または鍵ブロック４との間で認証が成立し、それぞれの鍵ブロックに格納された保存鍵を介した暗号処理を施したコンテンツが外部メモリに格納される。ここで、記録デバイスＡ，２１０４を記録再生器２１０２、または記録再生器２１０３に装着した場合、鍵ブロック１の保存鍵で暗号処理がなされたコンテンツは、記録再生器２１０２、記録再生器２１０３と鍵ブロック１との間での認証が成立しないので利用不可能となる。一方、鍵ブロック４の保存鍵で暗号処理がなされたコンテンツは、記録再生器２１０２、記録再生器２１０３と鍵ブロック４との間での認証が成立するので利用可能となる。

【０１８６】

上述のように、本発明のデータ処理装置においては、記録デバイスに複数の異なる鍵セットからなる鍵ブロックを構成し、一方、記録再生機器には、特定の鍵ブロックに対する認証可能なマスター鍵を格納する構成としたので、様々な利用態様に応じたコンテンツの利用制限を設定することが可能となる。

【０１８７】

なお、１つの記録再生機器において指定可能な鍵ブロックを複数、例えば１～ｋとし、他の記録再生器において指定可能な鍵ブロックをｐ～ｑのように複数とすることも可能であり、また、共通に利用可能な鍵ブロックを複数設ける構成としてもよい。

【０１８８】

（７）記録再生器から記録デバイスへのダウンロード処理

次に、本発明のデータ処理装置において、記録再生器３００から記録デバイス４００の外部メモリにコンテンツをダウンロードする処理について説明する。

【０１８９】

図２２は、記録再生器３００から記録デバイス４００へコンテンツをダウンロードする手順を説明する流れ図である。なお、図２２においては、既に記録再生器３００と記録デバイス４００との間で上述した相互認証処理が完了しているものとする。

【０１９０】

ステップＳ５１において、記録再生器３００の制御部３０１は、読み取り部３０４を使ってコンテンツを格納したメディア５００から所定のフォーマットに従ったデータを読み出すか、通信部３０５を使って通信手段６００から所定のフォーマットに従ってデータを受信する。そして、記録再生器３００の制御部３０１は、データの内のヘッダ（Header）部分（図４参照）を記録再生器３００の記録再生器暗号処理部３０２に送信する。

【０１９１】

次に、ステップＳ５２において、ステップＳ５１でヘッダ（Header）を受信した記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８にチェック値Ａを計算させる。チェック値Ａは、図２３に示すように、記録再生器暗号処理部３０２の内部メモリ３０７に保存されているチェック値Ａ生成鍵Ｋｉｃｖａを鍵とし、識別情報（Content ID）と取扱方針（Usage Policy）をメッセージとして図７で説明したＩＣＶ計算方法に従って計算される。なお、初期値は、ＩＶ＝０としても、記録再生器暗号処理部３０２の内部メモリ３０７にチェック値Ａ生成用初期値ＩＶａを保存しておき、それを使用してもよい。最後に、チェック値Ａとヘッダ（Header）内に格納されたチェック値：ＩＣＶａを比較し、一致していた場合にはステップＳ５３へ進む。

【０１９２】

先に図４において説明したようにチェック値Ａ，ＩＣＶａは、識別情報、取扱

方針の改竄を検証するためのチェック値である。記録再生器暗号処理部３０２の内部メモリ３０７に保存されているチェック値Ａ生成鍵Ｋｉｃｖａを鍵とし、識別情報（Content ID）と取扱方針（Usage Policy）をメッセージとして図７で説明したＩＣＶ計算方法に従って計算されるチェック値Ａが、ヘッダ（Header）内に格納されたチェック値：ＩＣＶａと一致した場合には、識別情報、取扱方針の改竄はないと判断される。

【０１９３】

次に、ステップＳ５３において、記録再生器暗号処理部３０２の制御部３０６は、配送鍵Ｋｄｉｓの生成を記録再生器暗号処理部３０２の暗号／復号化部３０８に行わせる。配送鍵Ｋｄｉｓの生成方法としては、例えば次のように生成する。

【０１９４】

【数４】

$$Kdis=DES(MKdis, ContentID \hat{} IVdis)$$

【０１９５】

ここで、ＭＫｄｉｓは、配送鍵Ｋｄｉｓを生成するための配送鍵用マスター鍵であり、これは、前述したように記録再生器３００の内部メモリに格納されている鍵である。またＣｏｎｔｅｎｔ　ＩＤはコンテンツデータのヘッダ部の識別情報であり、さらにＩＶｄｉｓは、配送鍵用初期値である。また、上記式において、ＤＥＳ（）は、第1引数を暗号鍵として、第２引数の値を暗号化する関数であり、演算＾は６４ビット単位の排他的論理和を示す。

【０１９６】

ステップＳ５４において、記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８を使って、ステップＳ５３で生成した配送鍵Ｋｄｉｓを用いて、読み取り部３０４を介して受信したメディア５００、または、通信部３０５を介して通信手段６００から受信したデータのヘッダ部に格納されたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎ（図４参照）の復号化処理を行う。図４に示されるようにこれらブロック情報鍵Ｋｂｉｔと

コンテンツ鍵Ｋｃｏｎは、ＤＶＤ，ＣＤ等のメディア、あるいはインターネット等の通信路上では、配送鍵Ｋｄｉｓによって予め暗号化処理が施されている。

【０１９７】

さらに、ステップＳ５５において、記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８を使って、ステップＳ５４で復号化したブロック情報鍵Ｋｂｉｔでブロック情報（ＢＩＴ）を復号化する。図４に示されるようにブロック情報（ＢＩＴ）は、ＤＶＤ，ＣＤ等のメディア、あるいはインターネット等の通信路上では、ブロック情報鍵Ｋｂｉｔによって予め暗号化処理が施されている。

【０１９８】

さらに、ステップＳ５６において、記録再生器暗号処理部３０２の制御部３０６は、ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎおよびブロック情報（ＢＩＴ）を８バイト単位に分割し、それら全てを排他的論理和する（加算、減算等、いずれの演算でもよい）。次に、記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８にチェック値Ｂ（ＩＣＶｂ）を計算させる。チェック値Ｂは、図２４に示すように、記録再生器暗号処理部３０２の内部メモリ３０７に保存されているチェック値Ｂ生成鍵Ｋｉｃｖｂを鍵とし、先ほど計算した排他的論理和値をＤＥＳで暗号化して生成する。最後に、チェック値ＢとHeader内のＩＣＶｂを比較し、一致していた場合にはステップＳ５７へ進む。

【０１９９】

先に図４において説明したように、チェック値Ｂ，ＩＣＶｂは、ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎ、ブロック情報（ＢＩＴ）の改竄を検証するためのチェック値である。記録再生器暗号処理部３０２の内部メモリ３０７に保存されているチェック値Ｂ生成鍵Ｋｉｃｖｂを鍵とし、ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎおよびブロック情報（ＢＩＴ）を８バイト単位に分割し排他的論理和して得られる値をＤＥＳで暗号化して生成したチェック値Ｂが、ヘッダ（Header）内に格納されたチェック値：ＩＣＶｂと一致した場合には、ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎ、ブロック情報の改竄はないと判断

される。

【０２００】

ステップＳ５７において、記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８に中間チェック値の計算をさせる。中間チェック値は、図２５に示すように、記録再生器暗号処理部３０２の内部メモリ３０７に保存されている総チェック値生成鍵Ｋｉｃｖｔを鍵とし、検証したヘッダ（Header）内のチェック値Ａ、チェック値Ｂ、保持しておいた全てのコンテンツチェック値をメッセージとして図７で説明したＩＣＶ計算方法に従って計算する。なお、初期値ＩＶ=0としても、記録再生器暗号処理部３０２の内部メモリ３０７に総チェック値生成用初期値ＩＶｔを保存しておき、それを使用してもよい。また、生成した中間チェック値は、必要に応じて記録再生器３００の記録再生器暗号処理部３０２に保持しておく。

【０２０１】

この中間チェック値は、チェック値Ａ、チェック値Ｂ、全てのコンテンツチェック値をメッセージとして生成されるものであり、これらの各チェック値の検証対象となっているデータについての検証を中間チェック値の照合処理によって行なってもよい。しかし、本実施例においては、システム全体の共有データとしての非改竄性検証処理と、ダウンロード処理後に各記録再生機器３００のみが占有する占有データとして識別するための検証処理を区別して実行可能とするために、中間チェック値からさらに複数の異なるチェック値、すなわち総チェック値ＩＣＶｔと、記録再生器固有チェック値ＩＣＶｄｅｖとを別々に、中間チェック値に基づいて生成可能としている。これらのチェック値については後段で説明する。

【０２０２】

記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８に総チェック値ＩＣＶｔの計算をさせる。総チェック値ＩＣＶｔは、図２５に示すように、記録再生器暗号処理部３０２の内部メモリ３０７に保存されているシステム署名鍵Ｋｓｙｓを鍵とし、中間チェック値をＤＥＳで暗号化して生成する。最後に、生成した総チェック値ＩＣＶｔとステップＳ

５１で保存しておいたHeader内のＩＣＶｔを比較し、一致していた場合には、ステップＳ５８へ進む。システム署名鍵Ｋｓｙｓは、複数の記録再生器、すなわちある一定のデータの記録再生処理を実行するシステム集合全体において共通する署名鍵である。

【０２０３】

先に図４において説明したように、総チェック値ＩＣＶｔは、ＩＣＶａ、ＩＣＶｂ、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。従って、上述の処理によって生成された総チェック値がヘッダ（Header）内に格納されたチェック値：ＩＣＶｔと一致した場合には、ＩＣＶａ、ＩＣＶｂ、各コンテンツブロックのチェック値全ての改竄はないと判断される。

【０２０４】

次に、ステップＳ５８において、記録再生器３００の制御部３０１は、ブロック情報（ＢＩＴ）内のコンテンツブロック情報を取り出し、コンテンツブロックが検証対象になっているかいないか調べる。コンテンツブロックが検証対象になっている場合には、ヘッダ中のブロック情報中にコンテンツチェック値が格納されている。

【０２０５】

コンテンツブロックが検証対象になっていた場合には、該当するコンテンツブロックを、記録再生器３００の読み取り部３０４を使ってメディア５００から読み出すか、記録再生器３００の通信部３０５を使って通信手段６００から受信し、記録再生器３００の記録再生器暗号処理部３０２へ送信する。これを受信した記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８にコンテンツ中間値を計算させる。

【０２０６】

コンテンツ中間値は、ステップＳ５４で復号化したコンテンツ鍵Ｋｃｏｎで、入力されたコンテンツブロックをＤＥＳのＣＢＣモードで復号化し、その結果を８バイトごとに区切り、全て排他的論理和（加算、減算等、いずれの演算でもよい）して生成する。

【０２０７】

次に、記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８にコンテンツチェック値の計算をさせる。コンテンツチェック値は、記録再生器暗号処理部３０２の内部メモリ３０７に保存されているコンテンツチェック値生成鍵Ｋｉｃｖｃを鍵とし、コンテンツ中間値をＤＥＳで暗号化して生成する。そして、記録再生器暗号処理部３０２の制御部３０６は、当該コンテンツチェック値と、ステップＳ５１で記録再生器３００の制御部３０１から受信したコンテンツブロック内のＩＣＶを比較し、その結果を記録再生器３００の制御部３０１に渡す。これを受信した記録再生器３００の制御部３０１は、検証に成功していた場合、次の検証対象コンテンツブロックを取り出して記録再生器３００の記録再生器暗号処理部３０２に検証させ、全てのコンテンツブロックを検証するまで同様の検証処理を繰り返す。なお、Ｈｅａｄｅｒ生成側と合わせておけば、ＩＶ＝０としても、記録再生器暗号処理部３０２の内部メモリ３０７にコンテンツチェック値生成用初期値ＩＶｃを保存しておき、それを使用してもよい。また、チェックした全てのコンテンツチェック値は、記録再生器３００の記録再生器暗号処理部３０２に保持しておく。さらにまた、記録再生器３００の記録再生器暗号処理部３０２は、検証対象のコンテンツブロックの検証順序を監視し、順序が間違っていたり、同一のコンテンツブロックを２回以上検証させられたりした場合には、認証に失敗したものとする。そして、全ての検証が成功した場合には、ステップＳ５９へ進む。

【０２０８】

次に、ステップＳ５９において、記録再生器３００の記録再生器暗号処理部３０２は、ステップＳ５４で復号化しておいたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎを、記録再生器暗号処理部３０２の暗号／復号化部３０８に、相互認証の際に共有しておいたセッション鍵Ｋｓｅｓで暗号化させる。記録再生器３００の制御部３０１は、セッション鍵Ｋｓｅｓで暗号化されたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎを記録再生器３００の記録再生器暗号処理部３０２から読み出し、これらのデータを記録再生器３００の記録デバイスコントローラ３０３を介して記録デバイス４００に送信する。

【０２０９】

次に、ステップＳ６０において、記録再生器３００から送信されてきたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎを受信した記録デバイス４００は、受信したデータを記録デバイス暗号処理部４０１の暗号／復号化部４０６に、相互認証の際に共有しておいたセッション鍵Ｋｓｅｓで復号化させ、記録デバイス暗号処理部４０１の内部メモリ４０５に保存してある記録デバイス固有の保存鍵Ｋｓｔｒで再暗号化させる。最後に、記録再生器３００の制御部３０１は、記録再生器３００の記録デバイスコントローラ３０３を介し、記録デバイス４００から保存鍵Ｋｓｔｒで再暗号化されたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎを読み出す。そして、これらの鍵を、配送鍵Ｋｄｉｓで暗号化されたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎに置き換える。

【０２１０】

ステップＳ６１において、記録再生器３００の制御部３０１は、データのヘッダ部の取扱方針（Usage Policy）から利用制限情報を取り出し、ダウンロードしたコンテンツが当該記録再生器３００のみで利用できる（この場合、利用制限情報が１に設定）か、別の同様な記録再生器３００でも利用できる（この場合、利用制限情報が０に設定）か判定する。判定の結果、利用制限情報が１であった場合には、ステップＳ６２に進む。

【０２１１】

ステップＳ６２において、記録再生器３００の制御部３０１は、記録再生器固有のチェック値を記録再生器３００の記録再生器暗号処理部３０２に計算させる。記録再生器固有のチェック値は、図２５に示すように記録再生器暗号処理部３０２の内部メモリ３０７に保存されている記録再生器署名鍵Ｋｄｅｖを鍵とし、ステップＳ５８で保持しておいた中間チェック値をＤＥＳで暗号化して生成する。計算された記録再生器固有のチェック値ＩＣＶｄｅｖは、総チェック値ＩＣＶｔの代わりに上書きされる。

【０２１２】

先に説明したように、システム署名鍵Ｋｓｙｓは、配信システムに共通の署名またはＩＣＶをつけるために使用するシステム署名鍵であり、また、記録再生器署名鍵Ｋｄｅｖは、記録再生器毎に異なり、記録再生器が署名またはＩＣＶをつ

けるために使用する記録再生器署名鍵である。すなわち、システム署名鍵Ｋｓｙｓによって署名されたデータは、同じシステム署名鍵を有するシステム（記録再生器）によってチェックが成功、すなわち総チェック値ＩＣＶｔが一致することになるので、共通に利用可能となるが、記録再生器署名鍵Ｋｄｅｖを用いて署名された場合には、記録再生器署名鍵はその記録再生器に固有の鍵であるので、記録再生器署名鍵Ｋｄｅｖを用いて署名されたデータ、すなわち、署名後、記録デバイスに格納されたデータは、他の記録再生器に、その記録デバイスを装着して再生しようとした場合、記録再生器固有のチェック値ＩＣＶｄｅｖが不一致となり、エラーとなるので再生できないことになる。

【０２１３】

従って、本発明のデータ処理装置においては、利用制限情報の設定によって、システムに共通に使用できるコンテンツ、記録再生器固有に利用できるコンテンツを自在に設定することが可能となる。

【０２１４】

ステップＳ６３において、記録再生器３００の制御部３０１は、コンテンツを記録デバイス４００の外部メモリ４０２に保存する。

【０２１５】

図２６は、利用制限情報が０の場合における記録デバイス内のコンテンツ状況を示す図である。図２７は、利用制限情報が１の場合における記録デバイス内のコンテンツ状況を示す図である。図２６が図４と異なる点は、コンテンツブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎが配送鍵Ｋｄｉｓで暗号化されているか、保存鍵Ｋｓｔｒで暗号化されているかだけである。また、図２７が図２６と異なる点は、中間チェック値から計算されるチェック値が、図２６ではシステム署名鍵Ｋｓｙｓで暗号化されているのに対し、図２７では記録再生器固有の記録再生器署名鍵Ｋｄｅｖで暗号化されていることである。

【０２１６】

なお、図２２の処理フローにおいて、ステップＳ５２でチェック値Ａの検証に失敗した場合、ステップＳ５６でチェック値Ｂの検証に失敗した場合、ステップＳ５７で総チェック値ＩＣＶｔの検証に失敗した場合、ステップＳ５８で各コン

テンツブロックのコンテンツチェック値の検証に失敗した場合には、ステップＳ６４に進み、所定のエラー表示を行う。

【０２１７】

また、ステップＳ６１で利用制限情報が０であった場合には、ステップＳ６２をスキップしてステップＳ６３へ進む。

【０２１８】

（８）記録デバイス格納情報の記録再生器での再生処理

次に記録デバイス４００の外部メモリ４０２に格納されたコンテンツ情報の記録再生器３００での再生処理について説明する。

【０２１９】

図２８は、記録再生器３００が記録デバイス４００からコンテンツを読み出し、コンテンツを利用する手順を説明する流れ図である。なお、図２８においても、既に記録再生器３００と記録デバイス４００との間で相互認証が完了しているものとする。

【０２２０】

ステップＳ７１において、記録再生器３００の制御部３０１は、記録デバイスコントローラ３０３を使って記録デバイス４００の外部メモリ４０２からコンテンツを読み出す。そして、記録再生器３００の制御部３０１は、データの内のヘッダ（Header）部分を記録再生器３００の記録再生器暗号処理部３０２に送信する。ステップＳ７２は、「（７）記録再生器から記録デバイスへのダウンロード処理」において説明したステップＳ５２と同様の処理であり、ヘッダ（Header）を受信した記録再生器暗号処理部３０２の制御部３０６が、記録再生器暗号処理部３０２の暗号／復号化部３０８にチェック値Ａを計算させる処理である。チェック値Ａは、先に説明した図２３に示すように記録再生器暗号処理部３０２の内部メモリ３０７に保存されているチェック値A生成鍵Ｋｉｃｖａを鍵とし、識別情報（Content ID）と取扱方針（Usage Policy）をメッセージとして図７で説明したと同様のＩＣＶ計算方法に従って計算される。

【０２２１】

先に説明したようにチェック値Ａ，ＩＣＶａは、識別情報、取扱方針の改竄を

検証するためのチェック値である。記録再生器暗号処理部３０２の内部メモリ３０７に保存されているチェック値Ａ生成鍵Ｋｉｃｖａを鍵とし、識別情報（Content ID）と取扱方針（Usage Policy）をメッセージとして図７で説明したICV計算方法に従って計算されるチェック値Ａが、ヘッダ（Header）内に格納されたチェック値：ＩＣＶａと一致した場合には、記録デバイス４００に格納された識別情報、取扱方針の改竄はないと判断される。

【０２２２】

次に、ステップＳ７３において、記録再生器３００の制御部３０１は、読み出したヘッダ（Header）部分からブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎを取り出し、記録再生器３００の記録デバイスコントローラ３０３を介して記録デバイス４００に送信する。記録再生器３００から送信されてきたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎを受信した記録デバイス４００は、受信したデータを記録デバイス暗号処理部４０１の暗号／復号化部４０６に、記録デバイス暗号処理部４０１の内部メモリ４０５に保存してある記録デバイス固有の保存鍵Ｋｓｔｒで復号化処理させ、相互認証の際に共有しておいたセッション鍵Ｋｓｅｓで再暗号化させる。そして、記録再生器３００の制御部３０１は、記録再生器３００の記録デバイスコントローラ３０３を介し、記録デバイス４００からセッション鍵Ｋｓｅｓで再暗号化されたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎを読み出す。

【０２２３】

次に、ステップＳ７４において、記録再生器３００の制御部３０１は、受信したセッション鍵Ｋｓｅｓで再暗号化されたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎを記録再生器３００の記録再生器暗号処理部３０２に送信する。

【０２２４】

セッション鍵Ｋｓｅｓで再暗号化されたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎを受信した記録再生器３００の記録再生器暗号処理部３０２は、記録再生器暗号処理部３０２の暗号／復号化部３０８に、セッション鍵Ｋｓｅｓで暗号化されたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎを、相互認証の際に共有しておいたセッション鍵Ｋｓｅｓで復号化させる。そして、復号化したブロ

ック情報鍵Ｋｂｉｔで、ステップＳ７１で受信しておいたブロック情報を復号化させる。

【０２２５】

なお、記録再生器３００の記録再生器暗号処理部３０２は、復号化したブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎおよびブロック情報ＢＩＴを、ステップＳ７１で受信しておいたブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎおよびブロック情報ＢＩＴに置き換えて保持しておく。また、記録再生器３００の制御部３０１は、復号化されたブロック情報ＢＩＴを記録再生器３００の記録再生器暗号処理部３０２から読み出しておく。

【０２２６】

ステップＳ７５は、「（７）記録再生器から記録デバイスへのダウンロード処理」において説明したステップＳ５６と同様の処理である。記録再生器暗号処理部３０２の制御部３０６が、記録デバイス４００から読み出したブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎおよびブロック情報（ＢＩＴ）を８バイト単位に分割し、それら全てを排他的論理和する。次に、記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８にチェック値Ｂ（ＩＣＶｂ）を計算させる。チェック値Ｂは、先に説明した図２４に示すように、記録再生器暗号処理部３０２の内部メモリ３０７に保存されているチェック値Ｂ生成鍵Ｋｉｃｖｂを鍵とし、先ほど計算した排他的論理和値をＤＥＳで暗号化して生成する。最後に、チェック値ＢとHeader内のＩＣＶｂを比較し、一致していた場合にはステップＳ７６へ進む。

【０２２７】

先に説明したように、チェック値Ｂ，ＩＣＶｂは、ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎ、ブロック情報の改竄を検証するためのチェック値である。記録再生器暗号処理部３０２の内部メモリ３０７に保存されているチェック値Ｂ生成鍵Ｋｉｃｖｂを鍵とし、記録デバイス４００から読み出したブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎおよびブロック情報（ＢＩＴ）を８バイト単位に分割し排他的論理和して得られる値をＤＥＳで暗号化して生成したチェック値Ｂが、記録デバイス４００から読み出したデータ中のヘッダ（Header）内に格

納されたチェック値：ＩＣＶｂと一致した場合には、記録デバイス４００に格納されたデータのブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎ、ブロック情報の改竄はないと判断される。

【０２２８】

ステップＳ７６において、記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８に中間チェック値の計算をさせる。中間チェック値は、先に説明した図２５に示すように記録再生器暗号処理部３０２の内部メモリ３０７に保存されている総チェック値生成鍵Ｋｉｃｖｔを鍵とし、検証したヘッダ（Header）内のチェック値Ａ、チェック値Ｂ、保持しておいた全てのコンテンツチェック値をメッセージとして図７他で説明したＩＣＶ計算方法に従って計算する。なお、初期値はＩＶ＝０としても、記録再生器暗号処理部３０２の内部メモリ３０７に総チェック値生成用初期値にＩＶｔを保存しておき、それを使用してもよい。また、生成した中間チェック値は、必要に応じて記録再生器３００の記録再生器暗号処理部３０２に保持しておく。

【０２２９】

次に、ステップＳ７７において、記録再生器３００の制御部３０１は、記録デバイス４００の外部メモリ４０２から読み出したデータのヘッダ部に含まれる取扱方針（Usage Policy）から利用制限情報を取り出し、ダウンロードしたコンテンツが当該記録再生器３００のみで利用できる（利用制限情報が１）か、別の同様な記録再生器３００でも利用できる（利用制限情報が０）か判定する。判定の結果、利用制限情報が１、すなわちダウンロードしたコンテンツが当該記録再生器３００のみで利用できる利用制限が設定されている場合には、ステップＳ８０に進み、利用制限情報が０、すなわち別の同様な記録再生器３００でも利用できる設定であった場合には、ステップＳ７８に進む。なお、ステップＳ７７の処理は、暗号処理部３０２が行なってもよい。

【０２３０】

ステップＳ７８においては、（７）記録再生器から記録デバイスへのダウンロード処理において説明したステップＳ５８と同様の総チェック値ＩＣＶｔの計算が実行される。すなわち、記録再生器暗号処理部３０２の制御部３０６は、記録

再生器暗号処理部３０２の暗号／復号化部３０８に総チェック値ＩＣＶｔの計算をさせる。総チェック値ＩＣＶｔは、先に説明した図２５に示すように記録再生器暗号処理部３０２の内部メモリ３０７に保存されているシステム署名鍵Ｋｓｙｓを鍵とし、中間チェック値をＤＥＳで暗号化して生成する。

【０２３１】

次に、ステップＳ７９に進み、ステップＳ７８において生成した総チェック値ＩＣＶｔとステップＳ７１で保存しておいたヘッダ（Header）内のＩＣＶｔを比較し、一致していた場合には、ステップＳ８２へ進む。

【０２３２】

先に説明したように、総チェック値ＩＣＶｔは、ＩＣＶａ、ＩＣＶｂ、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。従って、上述の処理によって生成された総チェック値がヘッダ（Header）内に格納されたチェック値：ＩＣＶｔと一致した場合には、記録デバイス４００に格納されたデータにおいて、ＩＣＶａ、ＩＣＶｂ、各コンテンツブロックのチェック値全ての改竄はないと判断される。

【０２３３】

ステップＳ７７での判定において、ダウンロードしたコンテンツが当該記録再生器３００のみで利用できる設定であった場合、すなわち設定情報が１であった場合は、ステップＳ８０に進む。

【０２３４】

ステップＳ８０において、記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８に、記録再生器固有のチェック値ＩＣＶｄｅｖの計算をさせる。記録再生器固有のチェック値ＩＣＶｄｅｖは、先に説明した図２５に示すように記録再生器暗号処理部３０２の内部メモリ３０７に保存されている記録再生器固有の記録再生器署名鍵Ｋｄｅｖを鍵とし、中間チェック値をＤＥＳで暗号化して生成する。ステップＳ８１において、ステップＳ８０で計算した記録再生器固有のチェック値ＩＣＶｄｅｖとステップＳ７１で保存しておいたHeader内のＩＣＶｄｅｖを比較し、一致していた場合には、ステップＳ８２へ進む。

【０２３５】

このように、システム署名鍵Ｋｓｙｓによって署名されたデータは、同じシステム署名鍵を有するシステム（記録再生器）によってチェックが成功、すなわち総チェック値ＩＣＶｔが一致することになるので共通に利用可能となり、記録再生器署名鍵Ｋｄｅｖを用いて署名された場合には、記録再生器署名鍵はその記録再生器に固有の鍵であるので、記録再生器署名鍵Ｋｄｅｖを用いて署名されたデータ、すなわち、署名後、記録デバイスに格納されたデータは、他の記録再生器に、その記録デバイスを装着して再生しようとした場合、記録再生器固有のチェック値ＩＣＶｄｅｖが不一致となり、エラーとなるので再生できないことになる。従って、利用制限情報の設定によって、システムに共通に使用できるコンテンツ、記録再生器固有に利用できるコンテンツを自在に設定することが可能となる。

【０２３６】

ステップＳ８２において、記録再生器３００の制御部３０１は、ステップＳ７４で読み出しておいたブロック情報ＢＩＴ内のコンテンツブロック情報を取り出し、コンテンツブロックが暗号化対象になっているかいないか調べる。暗号化対象になっていた場合には、該当するコンテンツブロックを、記録再生器３００の記録デバイスコントローラ３０３を介し、記録デバイス４００の外部メモリ４０２から読み出し、記録再生器３００の記録再生器暗号処理部３０２へ送信する。これを受信した記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８にコンテンツを復号化させるとともに、コンテンツブロックが検証対象になっている場合には次のステップＳ８３においてコンテンツチェック値を検証させる。

【０２３７】

ステップＳ８３は、「（７）記録再生器から記録デバイスへのダウンロード処理」において説明したステップＳ５８と同様の処理である。記録再生器３００の制御部３０１は、ブロック情報（ＢＩＴ）内のコンテンツブロック情報を取り出し、コンテンツブロックが検証対象になっているかいないかをコンテンツチェック値の格納状況から判定し、コンテンツブロックが検証対象になっていた場合に

は、該当するコンテンツブロックを、記録デバイス４００の外部メモリ４０２から受信し、記録再生器３００の記録再生器暗号処理部３０２へ送信する。これを受信した記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８にコンテンツ中間値を計算させる。

【０２３８】

コンテンツ中間値は、ステップＳ７４で復号化したコンテンツ鍵Ｋｃｏｎで、入力されたコンテンツブロックをＤＥＳのＣＢＣモードで復号化し、その結果を８バイトに区切り全て排他的論理和して生成する。

【０２３９】

次に、記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８にコンテンツチェック値の計算をさせる。コンテンツチェック値は、記録再生器暗号処理部３０２の内部メモリ３０７に保存されているコンテンツチェック値生成鍵Ｋｉｃｖｃを鍵とし、コンテンツ中間値をＤＥＳで暗号化して生成する。そして、記録再生器暗号処理部３０２の制御部３０６は、当該コンテンツチェック値と、ステップＳ７１で記録再生器３００の制御部３０１から受信したコンテンツブロック内のＩＣＶを比較し、その結果を記録再生器３００の制御部３０１に渡す。これを受信した記録再生器３００の制御部３０１は、検証に成功していた場合、次の検証対象コンテンツブロックを取り出して記録再生器３００の記録再生器暗号処理部３０２に検証させ、全てのコンテンツブロックを検証するまで同様の検証処理を繰り返す。なお、初期値はＩＶ＝０としても、記録再生器暗号処理部３０２の内部メモリ３０７にコンテンツチェック値生成用初期値ＩＶｃを保存しておき、それを使用してもよい。また、チェックした全てのコンテンツチェック値は、記録再生器３００の記録再生器暗号処理部３０２に保持しておく。さらにまた、記録再生器３００の記録再生器暗号処理部３０２は、検証対象のコンテンツブロックの検証順序を監視し、順序が間違っていたり、同一のコンテンツブロックを2回以上検証させられたりした場合には、認証に失敗したものとする。

【０２４０】

記録再生器３００の制御部３０１は、当該コンテンツチェック値の比較結果（

検証対象になっていない場合、比較結果は全て成功とする）を受信し、検証に成功していた場合には、記録再生器３００の記録再生器暗号処理部３０２から復号化されたコンテンツを取り出す。そして、次の復号化対象コンテンツブロックを取り出して記録再生器３００の記録再生器暗号処理部３０２に復号化させ、全てのコンテンツブロックを復号化するまで繰り返す。

【０２４１】

なお、ステップＳ８３において、記録再生器３００の記録再生器暗号処理部３０２は、コンテンツチェック値の検証処理において不一致となった場合には、検証失敗としてその時点で処理を中止し、残るコンテンツの復号化は行わない。また、記録再生器３００の記録再生器暗号処理部３０２は、復号化対象のコンテンツブロックの復号化順序を監視し、順序が間違っていたり、同一のコンテンツブロックを２回以上復号化させられたりした場合には、復号化に失敗したものとする。

【０２４２】

なお、ステップＳ７２でチェック値Ａの検証に失敗した場合、ステップＳ７５でチェック値Ｂの検証に失敗した場合、ステップＳ７９で総チェック値ＩＣＶｔの検証に失敗した場合、ステップＳ８１で記録再生器固有のチェック値ＩＣＶｄｅｖの検証に失敗した場合には、ステップＳ８３で各コンテンツブロックのコンテンツチェック値の検証に失敗した場合、ステップＳ８４に進み、所定のエラー表示を行う。

【０２４３】

以上説明してきたように、コンテンツをダウンロードしたり、利用したりする際に、重要なデータやコンテンツを暗号化しておいて隠蔽化したり、改竄検証ができるだけでなく、ブロック情報ＢＩＴを復号化するためのブロック情報鍵Ｋｂｉｔ、コンテンツを復号化するためのコンテンツ鍵Ｋｃｏｎが記録デバイス固有の保存鍵Ｋｓｔｒで保存されているため、単純に記録メディア上のデータを別の記録メディアに複製したとしても、コンテンツを正しく復号化することができなくすることができる。より具体的には、例えば図２８のステップＳ７４において、記録デバイス毎に異なる保存鍵Ｋｓｔｒで暗号化されたデータを復号化するた

め、別の記録デバイスではデータを正しく復号化できない構成を持つからである。

【０２４４】

（９）相互認証後の鍵交換処理

本発明のデータ処理装置における特徴の１つに、上述した記録再生器３００と記録デバイス４００との間で実行される相互認証処理の後においてのみ、記録デバイスの利用を可能とし、また、その利用態様を制限した点がある。

【０２４５】

例えば、不正な複製等によってコンテンツを格納したメモリカード等の記録デバイスを生成し、これを記録再生器にセットして利用されることを排除するために、記録再生器３００と、記録デバイス４００間での相互認証処理を実行し、かつ認証ＯＫとなったことを条件として、コンテンツ（暗号化された）の記録再生器３００および記録デバイス４００間での転送を可能としている。

【０２４６】

上記の制限的処理を実現するために、本発明のデータ処理装置においては、記録デバイス４００の暗号処理部４０１での処理は、すべて、予め設定されたコマンド列に基づいて実行される構成となっている。すなわち、記録デバイスは、コマンド番号に基づくコマンドを順次レジスタから取り出して実行するコマンド処理構成を持つ。この記録デバイスでのコマンド処理構成を説明する図を図２９に示す。

【０２４７】

図２９に示すように記録再生器暗号処理部３０２を有する記録再生器３００と記録デバイス暗号処理部４０１を有する記録デバイス４００間においては、記録再生器３００の制御部３０１の制御のもとに記録デバイスコントローラ３０３から記録デバイス４００の通信部(受信レジスタを含む)４０４に対してコマンド番号（Ｎｏ．）が出力される。

【０２４８】

記録デバイス４００は、暗号処理部４０１内の制御部４０３にコマンド番号管理部２２０１を有する。コマンド番号管理部２９０１は、コマンドレジスタ２９

０２を保持しており、記録再生器３００から出力されるコマンド番号に対応するコマンド列を格納している。コマンド列は、図２９の右に示すようにコマンド番号０からｙまで順次、コマンド番号に対して実行コマンドが対応付けされている。コマンド番号管理部２９０１は、記録再生器３００から出力されるコマンド番号を監視し、対応するコマンドをコマンドレジスタ２９０２から取り出して実行する。

【０２４９】

コマンドレジスタ２９０２に格納されたコマンドシーケンスは、図２９の右に示すように、認証処理シーケンスに関するコマンド列が先行するコマンド番号０～ｋに対応付けられている。さらに、認証処理シーケンスに関するコマンド列の後のコマンド番号ｐ～ｓに復号、鍵交換、暗号処理コマンドシーケンス１、さらに、後続するコマンド番号ｕ～ｙに復号、鍵交換、暗号処理コマンドシーケンス２が対応付けされている。

【０２５０】

先に図２０の認証処理フローにおいて説明したように、記録デバイス４００が記録再生器３００に装着されると、記録再生器３００の制御部３０１は、記録デバイスコントローラ３０３を介して記録デバイス４００に初期化命令を送信する。これを受信した記録デバイス４００は、記録デバイス暗号処理部４０１の制御部４０３において、通信部４０４を介して命令を受信し、認証フラグ２９０３をクリアする。すなわち未認証状態に設定する。または、記録再生器３００から記録デバイス４００に電源が供給される様な場合には、パワーオン時に未承認状態としてセットを行なう方式でもよい。

【０２５１】

次に、記録再生器３００の制御部３０１は、記録再生器暗号処理部３０２に初期化命令を送信する。このとき、記録デバイス挿入口番号も併せて送信する。記録デバイス挿入口番号を送信することにより、記録再生器３００に複数の記録デバイスが接続された場合であっても同時に複数の記録デバイス４００との認証処理、およびデータ送受信が可能となる。

【０２５２】

初期化命令を受信した記録再生器３００の記録再生器暗号処理部３０２は、記録再生器暗号処理部３０２の制御部において、記録デバイス挿入口番号に対応する認証フラグ２９０４をクリアする。すなわち未認証状態に設定する。

【０２５３】

これらの初期化処理が完了すると、記録再生器３００の制御部３０１は、記録デバイスコントローラ３０３を介してコマンド番号０から順次コマンド番号を昇順に出力する。記録デバイス４００のコマンド番号管理部２９０１は、記録再生器３００から入力されるコマンド番号を監視し、０から順次入力されることを確認して、対応するコマンドをコマンドレジスタ２９０２から取り出して認証処理等各種処理を実行する。入力されるコマンド番号が規定の順でなかった場合には、エラーとし、コマンド番号受付値を初期状態、すなわち実行可能コマンド番号＝０にリセットする。

【０２５４】

図２９に示すようにコマンドレジスタ２９０２に格納されたコマンドシーケンスは、認証処理を先行して処理するようにコマンド番号が付与されており、その後の処理に復号、鍵交換、暗号化処理の処理シーケンスが格納されている。

【０２５５】

復号、鍵交換、暗号化処理の処理シーケンスの具体例を図３０，３１を用いて説明する。

【０２５６】

図３０は、先に図２２において説明した記録再生器３００から記録デバイス４００へのコンテンツのダウンロード処理において実行される処理の一部を構成するものである。具体的には図２２におけるステップＳ５９～Ｓ６０の間で実行される

【０２５７】

図３０において、ステップＳ３００１は、記録再生器からセッション鍵Ｋｓｅｓで暗号化されたデータ（ｅｘ．ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎ）を記録デバイスが受信する処理であり、その後、前述の図２９で示したコマンド列ｐ～ｓが開始される。コマンド列ｐ～ｓは認証処理コマンド０～ｋが完了

し、図２９に示す認証フラグ２９０３，２９０４に認証済みのフラグがセットされた後開始される。これは、コマンド番号管理部２９０１がコマンド番号を０から昇順でのみ受け付けることによって保証される。

【０２５８】

ステップＳ３００２は、記録デバイスが記録再生器から受信したセッション鍵Ｋｓｅｓで暗号化されたデータ（ｅｘ．ブロック情報鍵Ｋｂｉｔ，コンテンツ鍵Ｋｃｏｎ）をレジスタに格納する処理である。

【０２５９】

ステップＳ３００３は、セッション鍵Ｋｓｅｓで暗号化されたデータ（ｅｘ．ブロック情報鍵Ｋｂｉｔ，コンテンツ鍵Ｋｃｏｎ）をレジスタから取り出してセッション鍵Ｋｓｅｓで復号する処理を実行するステップである。

【０２６０】

ステップＳ３００４は、セッション鍵Ｋｓｅｓで復号化されたデータ（ｅｘ．ブロック情報鍵Ｋｂｉｔ，コンテンツ鍵Ｋｃｏｎ）を保存鍵Ｋｓｔｒで暗号化する処理を実行するステップである。

【０２６１】

上記の処理ステップ３００２～３００４は、先の図２９で説明したコマンドレジスタ中のコマンド番号ｐ～ｓに含まれる処理である。これらの処理は、記録デバイス４００のコマンド番号管理部２９０１において記録再生器３００から受信するコマンド番号ｐ～ｓに従って記録デバイス暗号処理部４０１が順次実行する。

【０２６２】

次のステップＳ３００５は、保存鍵Ｋｓｔｒで暗号化したデータ（ｅｘ．ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎ）を記録デバイスの外部メモリに格納するステップである。このステップにおいては、記録デバイス暗号処理部４０１から記録再生器３００が保存鍵Ｋｓｔｒで暗号化したデータを読み出して、その後に記録デバイス４００の外部メモリ４０２に格納してもよい。

【０２６３】

上述のステップＳ３００２～Ｓ３００４は、連続して実行される割込み不可能

な実行シーケンスであり、たとえば、ステップＳ３００３の復号処理終了時点で、記録再生器３００からのデータ読み出し命令があったとしても、その読み出しコマンドは、コマンドレジスタ２９０２のコマンド番号ｐ～ｓに設定された昇順のコマンド番号とは異なるため、コマンド番号管理部２９０１は、読み出しの実行を受け付けない。従って、記録デバイス４００における鍵交換の際に発生する復号データを外部、例えば記録再生器３００から読み出すことは不可能となり、鍵データ、コンテンツの不正な読み出しを防止できる。

【０２６４】

図３１は、先に図２８において説明した記録デバイス４００からコンテンツを読み出して記録再生器３００において再生するコンテンツ再生処理において実行される処理の一部を構成するものである。具体的には図２８におけるステップＳ７３において実行される処理である。

【０２６５】

図３１において、ステップＳ３１０１は、記録デバイス４００の外部メモリ４０２から保存鍵Ｋｓｔｒで暗号化されたデータ（ｅｘ．ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎ）の読み出しを実行するステップである。

【０２６６】

ステップＳ３１０２は、記録デバイスのメモリから読み出した保存鍵Ｋｓｔｒで暗号化されたデータ（ｅｘ．ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎ）をレジスタに格納するステップである。このステップにおいては、記録デバイス４００の外部メモリ４０２から記録再生器３００が保存鍵Ｋｓｔｒで暗号化したデータを読み出して、その後に記録デバイス４００のレジスタに格納してもよい。

【０２６７】

ステップＳ３１０３は、保存鍵Ｋｓｔｒで暗号化されたデータ（ｅｘ．ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎ）をレジスタから取り出して保存鍵Ｋｓｔｒで復号処理するステップである。

【０２６８】

ステップＳ３１０４は、保存鍵Ｋｓｔｒで復号化されたデータ（ｅｘ．ブロッ

ク情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎ）をセッション鍵Ｋｓｅｓで暗号化処理するステップである。

【０２６９】

上記の処理ステップ３１０２～３１０４は、先の図２９で説明したコマンドレジスタ中のコマンド番号ｕ～ｙに含まれる処理である。これらの処理は、記録デバイスのコマンド番号管理部２９０１において記録再生器３００から受信するコマンド番号ｕ～ｙに従って記録デバイス暗号処理部４０６が順次実行する。

【０２７０】

次のステップＳ３１０５は、セッション鍵Ｋｓｅｓで暗号化したデータ（ｅｘ．ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎ）を記録デバイスから記録再生器へ送信する処理である。

【０２７１】

上述のステップＳ３１０２～Ｓ３１０４は、連続して実行される割込み不可能な実行シーケンスであり、たとえば、ステップＳ３１０３の復号処理終了時点で、記録再生器３００からのデータ読み出し命令があったとしても、その読み出しコマンドは、コマンドレジスタ２９０２のコマンド番号ｕ～ｙに設定された昇順のコマンド番号とは異なるため、コマンド番号管理部２９０１は、読み出しの実行を受け付けない。従って、記録デバイス４００における鍵交換の際に発生する復号データを外部、例えば記録再生器３００から読み出すことは不可能となり、鍵データあるいはコンテンツの不正な読み出しを防止できる。

【０２７２】

なお、図３０，３１に示す処理では、鍵交換によって復号、暗号化される対象が、ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎである例を示したが、これらの図２９に示したコマンドレジスタ２９０２に格納されたコマンドシーケンスには、コンテンツ自体の鍵交換を伴う復号、暗号化処理を含ませてもよく、鍵交換によって復号、暗号化される対象は上述の例に限定されるものではない。

【０２７３】

以上、本発明のデータ処理装置における相互認証後の鍵交換処理について説明した。このように、本発明のデータ処理装置における鍵交換処理は、記録再生器

と記録デバイス間での認証処理が終了した後においてのみ実行可能となり、さらに、鍵交換処理における復号データの外部からのアクセスが防止可能な構成となっているので、コンテンツ、鍵データの高度なセキュリティが確保される。

【０２７４】

（１０）複数のコンテンツデータフォーマットと、各フォーマットに対応するダウンロードおよび再生処理

上述した実施例では、例えば図３に示すメディア５００あるいは通信手段６００におけるデータフォーマットが図４に示す１つの種類である場合について説明してきた。しかしながら、メディア５００あるいは、通信手段６００におけるデータフォーマットは、上述の図４に示すフォーマットに限らず、コンテンツが音楽である場合、画像データである場合、ゲーム等のプログラムである場合等、コンテンツに応じたデータフォーマットを採用することが望ましい。以下、複数の異なるデータデータフォーマットと、各フォーマットに対応する記録デバイスへのダウンロード処理および記録デバイスからの再生処理について説明する。

【０２７５】

図３２～３５に４つの異なるデータフォーマットを示す。各図の左側には、図３に示すメディア５００、または通信手段６００上におけるデータフォーマットを、また各図の右側には記録デバイス４００の外部メモリ４０２に格納される場合のデータフォーマットを示してある。先に、図３２～３５に示すデータフォーマットの概略を説明し、その後、各フォーマットにおける各データの内容、および各フォーマットにおけるデータの差異について説明する。

【０２７６】

図３２は、フォーマットタイプ０であり、上述の説明中で例として示したタイプと共通のものである。このフォーマットタイプ０の特徴は、データ全体を任意の大きさのＮ個のデータブロック、すなわちブロック１～ブロックＮに分割し、各ブロックについて任意に暗号化し、暗号化ブロックと非暗号化ブロック、すなわち平文ブロックを混在させてデータを構成できる点である。ブロックの暗号化は、コンテンツ鍵Ｋｃｏｎによって実行されており、コンテンツ鍵Ｋｃｏｎは、メディア上では配送鍵Ｋｄｉｓによって暗号化され、記録デバイスにおける保存

時には、記録デバイスの内部メモリに格納された保存鍵Ｋｓｔｒによって暗号化される。ブロック情報鍵Ｋｂｉｔについてもメディア上では配送鍵Ｋｄｉｓによって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵Ｋｓｔｒによって暗号化される。これらの鍵交換は、前述の「（９）相互認証後の鍵交換処理」において説明した処理にしたがって実行される。

【０２７７】

図３３は、フォーマットタイプ１であり、このフォーマットタイプ１は、フォーマットタイプ０と同様、データ全体をＮ個のデータブロック、すなわちブロック１～ブロックＮに分割しているが、Ｎ個の各ブロックの大きさを同じ大きさとした点で前述のフォーマットタイプ０と異なる。コンテンツ鍵Ｋｃｏｎによるブロックの暗号化処理態様は前述のフォーマットタイプ０と同様である。また、メディア上で配送鍵Ｋｄｉｓによって暗号化され、記録デバイスにおける保存時には記録デバイスの内部メモリに格納された保存鍵Ｋｓｔｒによって暗号化されるコンテンツ鍵Ｋｃｏｎおよびブロック情報鍵Ｋｂｉｔ構成も上述のフォーマットタイプ０と同様である。フォーマットタイプ１は、フォーマットタイプ０と異なり、固定的なブロック構成としたことで、ブロック毎のデータ長等の構成データが簡略化されるので、フォーマットタイプ０に比較してブロック情報のメモリサイズを減らすことが可能となる。

【０２７８】

図３３の構成例では、各ブロックを暗号化パートと非暗号化（平文）パートの１組によって構成している。このようにブロックの長さ、構成が規則的であれば、復号処理等の際に各ブロック長、ブロック構成を確認する必要がなくなるので効率的な復号、暗号処理が可能となる。なお、フォーマット１においては、各ブロックを構成するパート、すなわち暗号化パート、非暗号化（平文）パートは、各パート毎にチェック対象として定義可能な構成となっており、要チェックパーツを含むブロックである場合は、そのブロックに関してコンテンツチェック値ＩＣＶｉが定義される。

【０２７９】

図３４は、フォーマットタイプ２であり、このフォーマットタイプ２の特徴は、同じ大きさのＮ個のデータブロック、すなわちブロック１～ブロックＮに分割され、各ブロックについて、それぞれ個別のブロック鍵Ｋｂｌｃで暗号化されていることである。各ブロック鍵Ｋｂｌｃの暗号化は、コンテンツ鍵Ｋｃｏｎによって実行されており、コンテンツ鍵Ｋｃｏｎは、メディア上では配送鍵Ｋｄｉｓによって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵Ｋｓｔｒによって暗号化される。ブロック情報鍵Ｋｂｉｔについてもメディア上では配送鍵Ｋｄｉｓによって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵Ｋｓｔｒによって暗号化される。

【０２８０】

図３５は、フォーマットタイプ３であり、このフォーマットタイプ３の特徴は、フォーマット・タイプ２と同様、同じ大きさのＮ個のデータブロック、すなわちブロック１～ブロックＮに分割され、各ブロックについて、それぞれ個別のブロック鍵Ｋｂｌｃで暗号化されていること、さらに、コンテンツ鍵を用いず、各ブロック鍵Ｋｂｌｃの暗号化は、メデイア上では配送鍵Ｋｄｉｓによって暗号化され、記録デバイス上では保存鍵Ｋｓｔｒによって暗号化されている点である。コンテンツ鍵Ｋｃｏｎは、メディア上、デバイス上、いずれにも存在しない。ブロック情報鍵Ｋｂｉｔはメディア上では配送鍵Ｋｄｉｓによって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵Ｋｓｔｒによって暗号化される。

【０２８１】

次に、上記フォーマットタイプ０～３のデータの内容について説明する。データは先に説明したように、ヘッダ部とコンテンツ部に大きく２つに分類され、ヘッダ部にはコンテンツ識別子、取扱方針、チェック値Ａ，Ｂ，総チェック値、ブロック情報鍵、コンテンツ鍵、ブロック情報が含まれる。

【０２８２】

取扱方針には、コンテンツのデータ長、ヘッダ長、フォーマットタイプ（以下説明するフォーマット０～３）、例えばプログラムであるか、データであるか等

のコンテンツタイプ、前述のコンテンツの記録デバイスへのダウンロード、再生の欄で説明したように、コンテンツが記録再生器固有に利用可能か否かを決定するフラグであるローカリゼーション・フラグ、さらに、コンテンツのコピー、ムーブ処理に関する許可フラグ、さらに、コンテンツ暗号化アルゴリズム、モード等、コンテンツに関する各種の利用制限情報および処理情報を格納する。

【０２８３】

チェック値Ａ：ＩＣＶａは、識別情報、取扱方針に対するチェック値であり、例えば、前述の図２３で説明した手法によって生成される。

【０２８４】

ブロック情報鍵Ｋｂｉｔは、ブロック情報を暗号化するための鍵であり、先に説明したように、メディア上では配送鍵Ｋｄｉｓによって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵Ｋｓｔｒによって暗号化される。

【０２８５】

コンテンツ鍵Ｋｃｏｎは、コンテンツの暗号化に用いる鍵であり、フォーマットタイプ０，１では、ブロック情報鍵Ｋｂｉｔと同様にメディア上では配送鍵Ｋｄｉｓによって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵Ｋｓｔｒによって暗号化される。なお、フォーマットタイプ２では、コンテンツ鍵Ｋｃｏｎは、コンテンツ各ブロックに構成されるブロック鍵Ｋｂｌｃの暗号化にも利用される。また、フォーマット・タイプ３においては、コンテンツ鍵Ｋｃｏｎは存在しない。

【０２８６】

ブロック情報は、個々のブロックの情報を記述するテーブルであり、ブロックの大きさ、暗号化されているか否かについてのフラグ、すなわち各ブロックがチェックの対象（ＩＣＶ）と、なっているか否かを示す情報が格納される。ブロックがチェックの対象となっている場合は、ブロックのチェック値ＩＣＶｉ（ブロックｉのチェック値）がテーブル中に定義されて格納される。このブロック情報は、ブロック情報暗号鍵Ｋｂｉｔによって暗号化される。

【０２８７】

なお、ブロックのチェック値、すなわちコンテンツチェック値ＩＣＶｉは、ブロックが暗号化されている場合、平文（復号文）全体を８バイト単位で排他論理和した値を記録再生器３００の内部メモリ３０７に格納されたコンテンツチェック値生成鍵Ｋｉｃｖｃで暗号化した値として生成される。また、ブロックが暗号化されていない場合は、ブロックデータ（平文）の全体を８バイト単位で図３６に示す改竄チェック値生成関数（ＤＥＳ－ＣＢＣ－ＭＡＣ、コンテンツチェック値生成鍵Ｋｉｃｖｃを鍵とする）に入力して得た値として生成される。図３６にコンテンツブロックのチェック値ＩＣＶｉを生成する構成例を示す。メッセージＭの各々が復号文データまたは平文データの各８バイトを構成する。

【０２８８】

なお、フォーマット・タイプ１においては、ブロック内のパーツのうち少なくとも１つがチェック値ＩＣＶｉの対象データ、すなわち要チェックパーツである場合は、そのブロックに関してコンテンツチェック値ＩＣＶｉが定義される。ブロックｉにおけるパーツｊのチェック値Ｐ－ＩＣＶｉｊは、パーツｊが暗号化されている場合、平文（復号文）全体を８バイト単位で排他論理和した値をコンテンツチェック値生成鍵Ｋｉｃｖｃで暗号化した値として生成される。また、パーツｊが暗号化されていない場合は、パーツのブロックのデータ（平文）の全体を８バイト単位で図３６に示す改竄チェック値生成関数（ＤＥＳ－ＣＢＣ－ＭＡＣ、コンテンツチェック値生成鍵Ｋｉｃｖｃを鍵とする）に入力して得た値として生成される。

【０２８９】

さらに、１つのブロックｉ内にチェツク対象であることを示す［ＩＣＶフラグ＝ｓｕｂｊｅｃｔ　ｏｆ　ＩＣＶ］であるパーツ、すなわち要チェックパーツが１つのみ存在する場合は、上述の手法で生成したチェック値Ｐ－ＩＣＶｉｊをそのままブロックのチェック値ＩＣＶｉとし、また、１つのブロックｉ内にチェツク対象であることを示す［ＩＣＶフラグ＝ｓｕｂｊｅｃｔ　ｏｆ　ＩＣＶ］であるパーツが複数存在する場合は、複数のパーツチェック値Ｐ－ＩＣＶｉｊをパーツ番号順に連結したデータを対象にして８バイト単位で図３７に示す改竄チェック値生成関数（ＤＥＳ－ＣＢＣ－ＭＡＣ、コンテンツチェック値生成鍵Ｋｉｃｖ

ｃを鍵とする）に入力して得た値として生成される。図３７にコンテンツブロックのコンテンツチェック値ＩＣＶｉを生成する構成例を示す。

【０２９０】

なお、フォーマット・タイプ２，３においては、ブロックのチェック値ＩＣＶｉは定義されない。

【０２９１】

チェック値Ｂ：ＩＣＶｂは、ブロック情報鍵、コンテンツ鍵、ブロック情報全体に対するチェック値であり、例えば、前述の図２４で説明した手法によって生成される。

【０２９２】

総チェック値ＩＣＶｔは、前述のチェック値Ａ：ＩＣＶａ、チェック値Ｂ：ＩＣＶｂ、さらにコンテンツのチェック対象となっている各ブロックに含まれるチェック値ＩＣＶｉ全体に対するチェック値であり、前述の図２５で説明したようにチェック値Ａ：ＩＣＶａ等の各チェック値から生成される中間チェック値にシステム署名鍵Ｋｓｙｓを適用して暗号化処理を実行することによって生成される。

【０２９３】

なお、フォーマット・タイプ２，３においては、総チェック値ＩＣＶｔは、前述のチェック値Ａ：ＩＣＶａ、チェック値Ｂ：ＩＣＶｂにコンテンツデータ、すなわちブロック１のブロック鍵から最終ブロックまでのコンテンツデータ全体を連結したデータから生成される中間チェック値にシステム署名鍵Ｋｓｙｓを適用して暗号化処理を実行することによって生成される。図３８にフォーマット・タイプ２，３における総チェック値ＩＣＶｔを生成する構成例を示す。

【０２９４】

固有チェック値ＩＣＶｄｅｖは、前述のローカリゼーションフラグが１にセットされている場合、すなわち、コンテンツが記録再生器固有に利用可能であることを示している場合に、総チェック値ＩＣＶｔに置き換えられるチェック値であり、フォーマット・タイプ０，１の場合は、前述のチェック値Ａ：ＩＣＶａ、チェック値Ｂ：ＩＣＶｂ、さらにコンテンツのチェック対象となっている各ブロッ

クに含まれるチェック値ＩＣＶｉ全体に対するチェック値として生成される。具体的には、前述の図２５、または図３８で説明したようにチェック値Ａ：ＩＣＶａ等の各チェック値から生成される中間チェック値に記録再生器署名鍵Ｋｄｅｖを適用して暗号化処理を実行することによって生成される。

【０２９５】

次にフォーマットタイプ０～３各々における記録再生器３００から記録デバイス４００に対するコンテンツのダウンロード処理、および記録再生器３００における記録デバイス４００からの再生処理について図３９～４４のフローを用いて説明する。

【０２９６】

まず、フォーマットタイプ０，１におけるコンテンツのダウンロード処理について図３９を用いて説明する。

【０２９７】

図３９に示す処理は、例えば図３に示す記録再生器３００に記録デバイス４００を装着することによって開始される。ステップＳ１０１は、記録再生器と記録デバイス間における認証処理ステップであり、先に説明した図２０の認証処理フローに従って実行される。

【０２９８】

ステップＳ１０１の認証処理が終了し、認証フラグがセットされると、記録再生器３００は、ステップＳ１０２において、例えばコンテンツデータを格納したメディア５００から、読み取り部３０４を介して所定のフォーマットに従ったデータを読み出すか、通信部３０５を使って通信手段６００から所定のフォーマットに従ってデータを受信し、記録再生器３００の制御部３０１が、データの内のヘッダ（Header）部分を記録再生器３００の記録再生器暗号処理部３０２に送信する。

【０２９９】

次に、ステップＳ１０３において、暗号処理部３０２の制御部３０６が記録再生器暗号処理部３０２の暗号／復号化部３０８にチェック値Ａを計算させる。チェック値Ａは、図２３に示すように、記録再生器暗号処理部３０２の内部メモリ

３０７に保存されているチェック値Ａ生成鍵Ｋｉｃｖａを鍵とし、識別情報（Content ID）と取扱方針（Usage Policy）をメッセージとして図７を用いて説明したＩＣＶ計算方法に従って計算される。次に、ステップＳ１０４において、チェック値Ａとヘッダ（Header）内に格納されたチェック値：ＩＣＶａを比較し、一致していた場合にはステップＳ１０５へ進む。

【０３００】

先に説明したようにチェック値Ａ，ＩＣＶａは、識別情報、取扱方針の改竄を検証するためのチェック値である。記録再生器暗号処理部３０２の内部メモリ３０７に保存されているチェック値Ａ生成鍵Ｋｉｃｖａを鍵とし、識別情報（Content ID）と取扱方針（Usage Policy）をメッセージとして、例えばＩＣＶ計算方法に従って計算されるチェック値Ａが、ヘッダ（Header）内に格納されたチェック値：ＩＣＶａと一致した場合には、識別情報、取扱方針の改竄はないと判断される。

【０３０１】

次に、ステップＳ１０５において、記録再生器暗号処理部３０２の制御部３０６は、配送鍵Ｋｄｉｓの取り出しまたは生成を記録再生器暗号処理部３０２の暗号／復号化部３０８に行わせる。配送鍵Ｋｄｉｓの生成方法は、先に説明した図２２のステップＳ５３と同様、例えば配送鍵用マスター鍵ＭＫｄｉｓを用いて行われる。

【０３０２】

次にステップＳ１０６において、記録再生器暗号処理部３０２の制御部３０６が、記録再生器暗号処理部３０２の暗号／復号化部３０８を使って、生成した配送鍵Ｋｄｉｓを用いて、読み取り部３０４を介して受信したメディア５００、または、通信部３０５を介して通信手段６００から受信したデータのヘッダ部に格納されたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎの復号化処理を行う。

【０３０３】

さらに、ステップＳ１０７において、記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８において、復号化したブロック情報鍵Ｋｂｉｔでブロック情報を復号化する。

【０３０４】

さらに、ステップＳ１０８において、記録再生器暗号処理部３０２の制御部３０６は、ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎおよびブロック情報（ＢＩＴ）から、チェック値Ｂ（ＩＣＶｂ’）を生成する。チェック値Ｂは、図２４に示すように、記録再生器暗号処理部３０２の内部メモリ３０７に保存されているチェック値Ｂ生成鍵Ｋｉｃｖｂを鍵とし、ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎおよびブロック情報（ＢＩＴ）からなる排他的論理和値をＤＥＳで暗号化して生成する。次に、ステップＳ１０９において、チェック値Ｂとヘッダ（Header）内のＩＣＶｂを比較し、一致していた場合にはステップＳ１１０へ進む。

【０３０５】

先に説明したように、チェック値Ｂ，ＩＣＶｂは、ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎ、ブロック情報の改竄を検証するためのチェック値である。記録再生器暗号処理部３０２の内部メモリ３０７に保存されているチェック値Ｂ生成鍵Ｋｉｃｖｂを鍵とし、ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎおよびブロック情報（ＢＩＴ）を８バイト単位に分割し排他的論理和して得られる値をＤＥＳで暗号化して生成したチェック値Ｂが、ヘッダ（Header）内に格納されたチェック値：ＩＣＶｂと一致した場合には、ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎ、ブロック情報の改竄はないと判断される。

【０３０６】

ステップＳ１１０において、記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８に中間チェック値の計算をさせる。中間チェック値は、図２５に示すように、記録再生器暗号処理部３０２の内部メモリ３０７に保存されている総チェック値生成鍵Ｋｉｃｖｔを鍵とし、検証したHeader内のチェック値Ａ、チェック値Ｂ、保持しておいた全てのコンテンツチェック値をメッセージとして図７他で説明したＩＣＶ計算方法に従って計算する。なお、生成した中間チェック値は、必要に応じて記録再生器３００の記録再生器暗号処理部３０２に保持しておく。

【０３０７】

次に、ステップＳ１１１において、記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８に総チェック値ＩＣＶｔ’の計算をさせる。総チェック値ＩＣＶｔ’は、図２５に示すように、記録再生器暗号処理部３０２の内部メモリ３０７に保存されているシステム署名鍵Ｋｓｙｓを鍵とし、中間チェック値をＤＥＳで暗号化して生成する。次に、ステップＳ１１２において、生成した総チェック値ＩＣＶｔ’とヘッダ（Header）内のＩＣＶｔを比較し、一致していた場合には、ステップＳ１１３へ進む。

【０３０８】

先に図４において説明したように、総チェック値ＩＣＶｔは、ＩＣＶａ、ＩＣＶｂ、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。従って、上述の処理によって生成された総チェック値がヘッダ（Header）内に格納されたチェック値：ＩＣＶｔと一致した場合には、ＩＣＶａ、ＩＣＶｂ、各コンテンツブロックのチェック値全ての改竄はないと判断される。

【０３０９】

次に、ステップＳ１１３において、記録再生器３００の制御部３０１は、ブロック情報（ＢＩＴ）内のコンテンツブロック情報を取り出し、コンテンツブロックが検証対象になっているかいないか調べる。コンテンツブロックが検証対象になっている場合には、ヘッダ中のブロック情報中にコンテンツチェック値が格納されている。

【０３１０】

コンテンツブロックが検証対象になっていた場合には、ステップＳ１１４において、該当するコンテンツブロックを、記録再生器３００の読み取り部３０４を使ってメディア５００から読み出すか、記録再生器３００の通信部３０５を使って通信手段６００から受信し、記録再生器３００の記録再生器暗号処理部３０２へ送信する。これを受信した記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８にコンテンツチェック値ＩＣＶｉ’を計算させる。

【０３１１】

コンテンツチェック値ＩＣＶｉ’は、先に説明したようにブロックが暗号化さ

れている場合、コンテンツ鍵Ｋｃｏｎで、入力されたコンテンツブロックをＤＥＳのＣＢＣモードで復号化し、その結果を全て８バイト単位で排他的論理和して生成したコンテンツ中間値を記録再生器３００の内部メモリ３０７に格納されたコンテンツチェック値生成鍵Ｋｉｃｖｃで暗号化して生成する。また、ブロックが暗号化されていない場合は、データ（平文）全体を８バイト単位で図３６に示す改竄チェック値生成関数（ＤＥＳ－ＣＢＣ－ＭＡＣ、コンテンツチェック値生成鍵Ｋｉｃｖｃを鍵とする）に入力して得た値として生成される。

【０３１２】

次にステップＳ１１５において、記録再生器暗号処理部３０２の制御部３０６は、当該コンテンツチェック値と、ステップＳ１０２で記録再生器３００の制御部３０１から受信したコンテンツブロック内のＩＣＶを比較し、その結果を記録再生器３００の制御部３０１に渡す。これを受信した記録再生器３００の制御部３０１は、検証に成功していた場合、次の検証対象コンテンツブロックを取り出して記録再生器３００の記録再生器暗号処理部３０２に検証させ、全てのコンテンツブロックを検証するまで同様の検証処理を繰り返す（ステップＳ１１６）。

【０３１３】

なお、ステップＳ１０４、ステップＳ１０９、ステップＳ１１２、ステップＳ１１５のいずれかにおいて、チェック値の一致が得られなかった場合はエラーとしてダウンロード処理は終了する。

【０３１４】

次に、ステップＳ１１７において、記録再生器３００の記録再生器暗号処理部３０２は、ステップＳ１０６で復号化したブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎを、記録再生器暗号処理部３０２の暗号／復号化部３０８に、相互認証の際に共有しておいたセッション鍵Ｋｓｅｓで暗号化させる。記録再生器３００の制御部３０１は、セッション鍵Ｋｓｅｓで暗号化されたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎを記録再生器３００の記録再生器暗号処理部３０２から読み出し、これらのデータを記録再生器３００の記録デバイスコントローラ３０３を介して記録デバイス４００に送信する。

【０３１５】

次に、ステップＳ１１８において、記録再生器３００から送信されてきたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎを受信した記録デバイス４００は、受信したデータを記録デバイス暗号処理部４０１の暗号／復号化部４０６に、相互認証の際に共有しておいたセッション鍵Ｋｓｅｓで復号化させ、記録デバイス暗号処理部４０１の内部メモリ４０５に保存してある記録デバイス固有の保存鍵Ｋｓｔｒで再び暗号化させ、記録再生器３００の制御部３０１は、記録再生器３００の記録デバイスコントローラ３０３を介し、記録デバイス４００から保存鍵Ｋｓｔｒで再暗号化されたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎを読み出す。すなわち、配送鍵Ｋｄｉｓで暗号化されたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎの鍵のかけかえを行なう。

【０３１６】

次に、ステップＳ１１９において、記録再生器３００の制御部３０１は、データのヘッダ部の取扱方針（Usage Policy）から利用制限情報を取り出し、ダウンロードしたコンテンツが当該記録再生器３００のみで利用できるか否かの判定を行なう。この判定は、ローカリゼーションフラグ（利用制限情報）＝１に設定されている場合は、ダウンロードしたコンテンツが当該記録再生器３００のみで利用でき、ローカリゼーションフラグ（利用制限情報）＝０に設定されている場合は、ダウンロードしたコンテンツが別の同様な記録再生器３００でも利用できることを示す。判定の結果、ローカリゼーションフラグ（利用制限情報）＝１であった場合には、ステップＳ１２０に進む。

【０３１７】

ステップＳ１２０において、記録再生器３００の制御部３０１は、記録再生器固有のチェック値を記録再生器３００の記録再生器暗号処理部３０２に計算させる。記録再生器固有のチェック値は、図２５に示すように記録再生器暗号処理部３０２の内部メモリ３０７に保存されている記録再生器に固有の記録再生器署名鍵Ｋｄｅｖを鍵とし、ステップＳ１１０で生成した中間チェック値をＤＥＳで暗号化して生成する。計算された記録再生器固有のチェック値ＩＣＶｄｅｖは、総チェック値ＩＣＶｔの代わりに上書きされる。

【０３１８】

先に説明したように、システム署名鍵Ｋｓｙｓは、配信システムに共通の署名またはICVをつけるために使用するシステム署名鍵であり、また、記録再生器署名鍵Ｋｄｅｖは、記録再生器毎に異なり、記録再生器が署名またはＩＣＶをつけるために使用する記録再生器署名鍵である。すなわち、システム署名鍵Ｋｓｙｓによって署名されたデータは、同じシステム署名鍵を有するシステム（記録再生器）によってチェックが成功、すなわち総チェック値ＩＣＶｔが一致することになるので、共通に利用可能となるが、記録再生器署名鍵Ｋｄｅｖを用いて署名された場合には、記録再生器署名鍵はその記録再生器に固有の鍵であるので、記録再生器署名鍵Ｋｄｅｖを用いて署名されたデータ、すなわち、署名後、記録デバイスに格納されたデータは、他の記録再生器に、その記録デバイスを装置して再生しようとした場合、記録再生器固有のチェック値ＩＣＶｄｅｖが不一致となり、エラーとなるので再生できないことになる。本発明のデータ処理装置においては、利用制限情報の設定によって、システムに共通に使用できるコンテンツ、記録再生器固有に利用できるコンテンツを自在に設定できるものである。

【０３１９】

次に、ステップＳ１２１において、記録再生器３００の制御部３０１は、記録再生器暗号処理部３０２に格納データフォーマットの形成を実行させる。先に説明したように、フォーマットタイプは０～３まで各タイプがあり、ヘッダ中の取扱方針（図５参照）中に設定され、この設定タイプにしたがって、先に説明した図３２～３５の右側の格納フォーマットにしたがってデータを形成する。この図３９に示すフローはフォーマット０，１のいずれかであるので、図３２，３３のいずれかのフォーマットに形成される。

【０３２０】

ステップＳ１２１において格納データフォーマットの形成が終了すると、ステップ１２２において、記録再生器３００の制御部３０１は、コンテンツを記録デバイス４００の外部メモリ４０２に保存する。

【０３２１】

以上が、フォーマットタイプ０，１におけるコンテンツデータのダウンロード処理の態様である。

【０３２２】

次に、フォーマットタイプ２におけるコンテンツデータのダウンロード処理について図４０を用いて説明する。上記したフォーマットタイプ０，１のダウンロード処理と異なる点を中心に説明する。

【０３２３】

ステップＳ１０１～Ｓ１０９は、上記したフォーマットタイプ０，１のダウンロード処理と同様であるので説明は省略する。

【０３２４】

フォーマットタイプ２は、先に説明したようにコンテンツチェック値ＩＣＶｉが定義されていないので、ブロック情報中には、コンテンツチェック値ＩＣＶｉを持たない。フォーマットタイプ２における中間チェック値は、図３８に示すようにチェック値Ａ、チェック値Ｂと、第１ブロックの先頭データ（ブロック１のブロック鍵）から最終ブロックまでのコンテンツデータ全体を連結したデータに基づいて生成される中間チェック値にシステム署名鍵Ｋｓｙｓを適用して暗号化処理を実行することによって生成される。

【０３２５】

従って、フォーマットタイプ２のダウンロード処理においては、ステップＳ１５１においてコンテンツデータを読み出し、ステップＳ１５２において、チェック値Ａ、チェック値Ｂと読み出したコンテンツデータに基づいて中間チェック値の生成を実行する。なお、コンテンツデータは暗号化されている場合でも、復号処理を行なわない。

【０３２６】

フォーマットタイプ２では、前述のフォーマットタイプ０，１での処理のようにブロックデータの復号、コンテンツチェック値の照会処理を行なわないので、迅速な処理が可能となる。

【０３２７】

ステップＳ１１１以下の処理は、フォーマットタイプ０，１における処理と同様であるので説明を省略する。

【０３２８】

以上が、フォーマットタイプ２におけるコンテンツデータのダウンロード処理の態様である。上述したようにフォーマットタイプ２のダウンロード処理は、フォーマットタイプ０，１での処理のようにブロックデータの復号、コンテンツチェック値の照会処理を行なわないので、迅速な処理が可能となり、音楽データ等リアルタイム処理が要求されるデータ処理に適したフォーマットである。

【０３２９】

次に、フォーマットタイプ３におけるコンテンツデータのダウンロード処理について図４１を用いて説明する。上記したフォーマットタイプ０，１，２のダウンロード処理と異なる点を中心に説明する。

【０３３０】

ステップＳ１０１～Ｓ１０５は、上記したフォーマットタイプ０，１，２のダウンロード処理と同様であるので説明は省略する。

【０３３１】

フォーマットタイプ３は、基本的にフォーマットタイプ２における処理と共通する部分が多いが、フォーマットタイプ３はコンテンツ鍵を有しておらず、またブロック鍵Ｋｂｌｃが記録デバイスにおいては保存鍵Ｋｓｔｒで暗号化されて格納される点がフォーマットタイプ２と異なる。

【０３３２】

フォーマットタイプ３のダウンロード処理におけるフォーマットタイプ２と相違する点を中心として説明する。フォーマットタイプ３では、ステップＳ１０５の次ステップであるステップＳ１６１において、ブロック情報鍵の復号を行なう。記録再生器暗号処理部３０２の制御部３０６が、記録再生器暗号処理部３０２の暗号／復号化部３０８を使って、ステップＳ１０５で生成した配送鍵Ｋｄｉｓを用いて、読み取り部３０４を介して受信したメディア５００、または、通信部３０５を介して通信手段６００から受信したデータのヘッダ部に格納されたブロック情報鍵Ｋｂｉｔの復号化処理を行う。フォーマットタイプ３では、データ中にコンテンツ鍵Ｋｃｏｎが存在しないため、コンテンツ鍵Ｋｃｏｎの復号化処理は実行されない。

【０３３３】

次のステップＳ１０７では、ステップＳ１６１で復号したブロック情報鍵Ｋｂｉｔを用いてブロック情報の復号が実行され、さらに、ステップＳ１６２において、記録再生器暗号処理部３０２の制御部３０６は、ブロック情報鍵Ｋｂｉｔ、およびブロック情報（ＢＩＴ）から、チェック値Ｂ（ＩＣＶｂ’）を生成する。チェック値Ｂは、記録再生器暗号処理部３０２の内部メモリ３０７に保存されているチェック値Ｂ生成鍵Ｋｉｃｖｂを鍵とし、ブロック情報鍵Ｋｂｉｔ、およびブロック情報（ＢＩＴ）からなる排他的論理和値をＤＥＳで暗号化して生成する。次に、ステップＳ１０９において、チェック値Ｂとヘッダ（Header）内のＩＣＶｂを比較し、一致していた場合にはステップＳ１５１へ進む。

【０３３４】

フォーマットタイプ３では、チェック値Ｂ，ＩＣＶｂは、ブロック情報鍵Ｋｂｉｔ、ブロック情報の改竄を検証するためのチェック値として機能する。生成したチェック値Ｂが、ヘッダ（Header）内に格納されたチェック値：ＩＣＶｂと一致した場合には、ブロック情報鍵Ｋｂｉｔ、ブロック情報の改竄はないと判断される。

【０３３５】

ステップＳ１５１～Ｓ１１２は、フォーマットタイプ２の処理と同様であるので説明を省略する。

【０３３６】

ステップＳ１６３では、ステップＳ１５１で読み出したコンテンツデータに含まれるブロック鍵ＫｂｌｃをステップＳ１０５で生成した配送鍵Ｋｄｉｓによって復号する。

【０３３７】

次にステップＳ１６４では、記録再生器３００の記録再生器暗号処理部３０２が、ステップＳ１６１で復号化したブロック情報鍵Ｋｂｉｔと、ステップＳ１６３で復号したブロック鍵Ｋｂｌｃを、記録再生器暗号処理部３０２の暗号／復号化部３０８に、相互認証の際に共有しておいたセッション鍵Ｋｓｅｓで暗号化させる。記録再生器３００の制御部３０１は、セッション鍵Ｋｓｅｓで暗号化されたブロック情報鍵Ｋｂｉｔとブロック鍵Ｋｂｌｃを記録再生器３００の記録再生

器暗号処理部３０２から読み出し、これらのデータを記録再生器３００の記録デバイスコントローラ３０３を介して記録デバイス４００に送信する。

【０３３８】

次に、ステップＳ１６５において、記録再生器３００から送信されてきたブロック情報鍵Ｋｂｉｔとブロック鍵Ｋｂｌｃを受信した記録デバイス４００は、受信したデータを記録デバイス暗号処理部４０１の暗号／復号化部４０６に、相互認証の際に共有しておいたセッション鍵Ｋｓｅｓで復号化させ、記録デバイス暗号処理部４０１の内部メモリ４０５に保存してある記録デバイス固有の保存鍵Ｋｓｔｒで再暗号化させ、記録再生器３００の制御部３０１は、記録再生器３００の記録デバイスコントローラ３０３を介し、記録デバイス４００から保存鍵Ｋｓｔｒで再暗号化されたブロック情報鍵Ｋｂｉｔとブロック鍵Ｋｂｌｃを読み出す。すなわち、当初、配送鍵Ｋｄｉｓで暗号化されたブロック情報鍵Ｋｂｉｔとブロック鍵Ｋｂｌｃを保存鍵Ｋｓｔｒで再暗号化されたブロック情報鍵Ｋｂｉｔとブロック鍵Ｋｂｌｃへ置き換えを行なう。

【０３３９】

以下のステップＳ１１９～Ｓ１２２は、前述のフォーマットタイプ０，１，２と同様であるので説明を省略する。

【０３４０】

以上が、フォーマットタイプ３におけるコンテンツデータのダウンロード処理の態様である。上述したようにフォーマットタイプ３のダウンロード処理は、フォーマットタイプ２と同様、ブロックデータの復号、コンテンツチェック値の照会処理を行なわないので、迅速な処理が可能となり、音楽データ等リアルタイム処理が要求されるデータ処理に適したフォーマットである。また、ブロック鍵Ｋｂｌｃにより暗号化コンテンツを保護する範囲が局所化されているので、フォーマットタイプ２に比較して、よりセキュリティが高度となる。

【０３４１】

次に、フォーマットタイプ０～３各々における記録再生器３００における記録デバイス４００からの再生処理について図４２～４５のフローを用いて説明する。

【０３４２】

まず、フォーマットタイプ０におけるコンテンツの再生処理について図４２を用いて説明する。

【０３４３】

ステップＳ２０１は、記録再生器と記録デバイス間における認証処理ステップであり、先に説明した図２０の認証処理フローに従って実行される。

【０３４４】

ステップＳ２０１の認証処理が終了し、認証フラグがセットされると、記録再生器３００は、ステップＳ２０２において、記録デバイス４００から所定のフォーマットに従ったデータのヘッダを読み出し、記録再生器３００の記録再生器暗号処理部３０２に送信する。

【０３４５】

次に、ステップＳ２０３において、暗号処理部３０２の制御部３０６が記録再生器暗号処理部３０２の暗号／復号化部３０８にチェック値Ａを計算させる。チェック値Ａは、先に説明した図２３に示すように、記録再生器暗号処理部３０２の内部メモリ３０７に保存されているチェック値Ａ生成鍵Ｋｉｃｖａを鍵とし、識別情報（Content ID）と取扱方針（Usage Policy）をメッセージとして計算される。次に、ステップＳ２０４において、計算されたチェック値Ａとヘッダ（Header）内に格納されたチェック値：ＩＣＶａを比較し、一致していた場合にはステップＳ２０５へ進む。

【０３４６】

チェック値Ａ，ＩＣＶａは、識別情報、取扱方針の改竄を検証するためのチェック値である。計算されたチェック値Ａが、ヘッダ（Header）内に格納されたチェック値：ＩＣＶａと一致した場合には、記録デバイス４００に格納された識別情報、取扱方針の改竄はないと判断される。

【０３４７】

次に、ステップＳ２０５において、記録再生器３００の制御部３０１は、読み出したヘッダから記録デバイス固有の保存鍵Ｋｓｔｒで暗号化されたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎを取り出し、記録再生器３００の記録デバ

イスコントローラ３０３を介して記録デバイス４００に送信する。

【０３４８】

記録再生器３００から送信されてきたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎを受信した記録デバイス４００は、受信したデータを記録デバイス暗号処理部４０１の暗号／復号化部４０６に、記録デバイス暗号処理部４０１の内部メモリ４０５に保存してある記録デバイス固有の保存鍵Ｋｓｔｒで復号化処理させ、相互認証の際に共有しておいたセッション鍵Ｋｓｅｓで再び暗号化させる。この処理は、前述した（９）相互認証後の鍵交換処理の欄で詳しく述べた通りである。

【０３４９】

ステップＳ２０６では、記録再生器３００の制御部３０１は、記録再生器３００の記録デバイスコントローラ３０３を介し、記録デバイス４００からセッション鍵Ｋｓｅｓで再暗号化されたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎを受信する。

【０３５０】

次に、ステップＳ２０７において、記録再生器３００の制御部３０１は、受信したセッション鍵Ｋｓｅｓで再暗号化されたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎを記録再生器３００の記録再生器暗号処理部３０２に送信し、セッション鍵Ｋｓｅｓで再暗号化されたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎを受信した記録再生器３００の記録再生器暗号処理部３０２は、記録再生器暗号処理部３０２の暗号／復号化部３０８に、セッション鍵Ｋｓｅｓで暗号化されたブロック情報鍵Ｋｂｉｔとコンテンツ鍵Ｋｃｏｎを、相互認証の際に共有しておいたセッション鍵Ｋｓｅｓで復号化させる。

【０３５１】

さらに、ステップＳ２０８において、復号化したブロック情報鍵Ｋｂｉｔで、ステップＳ２０２で読み出しておいたブロック情報を復号化する。なお、記録再生器３００の記録再生器暗号処理部３０２は、復号化したブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎおよびブロック情報ＢＩＴを、ステップＳ２０２で読み出したヘッダに含まれるブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎおよ

びブロック情報ＢＩＴに置き換えて保持しておく。また、記録再生器３００の制御部３０１は、復号化されたブロック情報ＢＩＴを記録再生器３００の記録再生器暗号処理部３０２から読み出しておく。

【０３５２】

さらに、ステップＳ２０９において、記録再生器暗号処理部３０２の制御部３０６は、ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎおよびブロック情報（ＢＩＴ）から、チェック値Ｂ（ＩＣＶｂ’）を生成する。チェック値Ｂは、図２４に示すように、記録再生器暗号処理部３０２の内部メモリ３０７に保存されているチェック値Ｂ生成鍵Ｋｉｃｖｂを鍵とし、ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎおよびブロック情報（ＢＩＴ）からなる排他的論理和値をＤＥＳで暗号化して生成する。次に、ステップＳ２１０において、チェック値Ｂとヘッダ（Header）内のＩＣＶｂを比較し、一致していた場合にはステップＳ２１１へ進む。

【０３５３】

チェック値Ｂ，ＩＣＶｂは、ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎ、ブロック情報の改竄を検証するためのチェック値であり、生成したチェック値Ｂが、ヘッダ（Header）内に格納されたチェック値：ＩＣＶｂと一致した場合には、記録デバイス４００に保存されたデータ中のブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎ、ブロック情報の改竄はないと判断される。

【０３５４】

ステップＳ２１１において、記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８に中間チェック値の計算をさせる。中間チェック値は、図２５に示すように、記録再生器暗号処理部３０２の内部メモリ３０７に保存されている総チェック値生成鍵Ｋｉｃｖｔを鍵とし、検証したHeader内のチェック値Ａ、チェック値Ｂ、ブロック情報中の全てのコンテンツチェック値をメッセージとして図７他で説明したＩＣＶ計算方法に従って計算する。なお、生成した中間チェック値は、必要に応じて記録再生器３００の記録再生器暗号処理部３０２に保持しておく。

【０３５５】

次に、ステップＳ２１２において、記録再生器３００の制御部３０１は、記録デバイス４００の外部メモリ４０２から読み出したデータのヘッダ部に含まれる取扱方針（Usage Policy）から利用制限情報を取り出し、再生予定のコンテンツが当該記録再生器３００のみで利用できる（利用制限情報が１）か、別の同様な記録再生器３００でも利用できる（利用制限情報が０）か判定する。判定の結果、利用制限情報が１、すなわち再生コンテンツが当該記録再生器３００のみで利用できる利用制限が設定されている場合には、ステップＳ２１３に進み、利用制限情報が０、すなわち別の同様な記録再生器３００でも利用できる設定であった場合には、ステップＳ２１５に進む。なお、ステップＳ２１２の処理は暗号処理部３０２が行なってもよい。

【０３５６】

ステップＳ２１３では、記録再生器３００の制御部３０１は、記録再生器固有のチェック値ＩＣＶｄｅｖ’を記録再生器３００の記録再生器暗号処理部３０２に計算させる。記録再生器固有のチェック値ＩＣＶｄｅｖ’は、図２５に示すように記録再生器暗号処理部３０２の内部メモリ３０７に保存されている記録再生器署名鍵Ｋｄｅｖを鍵とし、ステップＳ２１１で保持しておいた中間チェック値をＤＥＳで暗号化して生成する。

【０３５７】

次に、ステップＳ２１４において、ステップＳ２１３で計算した記録再生器固有のチェック値ＩＣＶｄｅｖ’とステップＳ２０２で読み出したヘッダ内のＩＣＶｄｅｖを比較し、一致していた場合には、ステップＳ２１７へ進む。

【０３５８】

一方ステップＳ２１５では、記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８に総チェック値ＩＣＶｔの計算をさせる。総チェック値ＩＣＶｔ’は、図２５に示すように、記録再生器暗号処理部３０２の内部メモリ３０７に保存されているシステム署名鍵Ｋｓｙｓを鍵とし、中間チェック値をＤＥＳで暗号化して生成する。次に、ステップＳ２１６において、生成した総チェック値ＩＣＶｔ’とヘッダ（Header）内のＩＣＶｔを比較し、一致していた場合には、ステップＳ２１７へ進む。

【０３５９】

総チェック値ＩＣＶｔ、および記録再生器固有のチェック値ＩＣＶｄｅｖは、ＩＣＶａ、ＩＣＶｂ、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。従って、上述の処理によって生成されたチェック値がヘッダ（Header）内に格納されたチェック値：ＩＣＶｔまたはＩＣＶｄｅｖと一致した場合には、記録デバイス４００に格納されたＩＣＶａ、ＩＣＶｂ、各コンテンツブロックのチェック値全ての改竄はないと判断される。

【０３６０】

次に、ステップＳ２１７において、記録再生器３００の制御部３０１は、記録デバイス４００からブロックデータを読み出す。さらに、ステップＳ２１８において暗号化されているか否かを判定し、暗号化されている場合は、記録再生器３００の暗号処理部３０２においてブロックデータの復号を行なう。暗号化されていない場合は、ステップＳ２１９をスキップしてステップＳ２２０に進む。

【０３６１】

次に、ステップＳ２２０において、記録再生器３００の制御部３０１は、ブロック情報（ＢＩＴ）内のコンテンツブロック情報に基づいて、コンテンツブロックが検証対象になっているかいないか調べる。コンテンツブロックが検証対象になっている場合には、ヘッダ中のブロック情報中にコンテンツチェック値が格納されている。コンテンツブロックが検証対象になっていた場合には、ステップＳ２２１において、該当するコンテンツブロックのコンテンツチェック値ＩＣＶｉ’を計算させる。コンテンツブロックが検証対象になっていない場合には、ステップＳ２２１とＳ２２２をスキップしてステップＳ２２３に進む。

【０３６２】

コンテンツチェック値ＩＣＶｉ’は、先に図３６で説明したようにブロックが暗号化されている場合、コンテンツ鍵Ｋｃｏｎで、入力されたコンテンツブロックをＤＥＳのＣＢＣモードで復号化し、その結果を全て８バイト単位で排他的論理和して生成したコンテンツ中間値を記録再生器３００の内部メモリ３０７に格納されたコンテンツチェック値生成鍵Ｋｉｃｖｃで暗号化して生成する。また、ブロックが暗号化されていない場合は、データ（平文）全体を８バイト単位で図

３６に示す改竄チェック値生成関数（ＤＥＳ－ＣＢＣ－ＭＡＣ、コンテンツチェック値生成鍵Ｋｉｃｖｃを鍵とする）に入力して得た値として生成される。

【０３６３】

ステップＳ２２２においては、記録再生器暗号処理部３０２の制御部３０６は、生成したコンテンツチェック値ＩＣＶｉ’と、ステップＳ２０２で記録デバイス４００から受信したヘッダ部に格納されたコンテンツチェック値ＩＣＶｉとを比較し、その結果を記録再生器３００の制御部３０１に渡す。これを受信した記録再生器３００の制御部３０１は、検証に成功していた場合、ステップＳ２２３において、記録再生器システムＲＡＭ上に実行(再生)用コンテンツ平文データを格納する。記録再生器３００の制御部３０１は、さらに次の検証対象コンテンツブロックを取り出して記録再生器３００の記録再生器暗号処理部３０２に検証させ、全てのコンテンツブロックを検証するまで同様の検証処理、ＲＡＭ格納処理を繰り返す（ステップＳ２２４）。

【０３６４】

なお、ステップＳ２０４、ステップＳ２１０、ステップＳ２１４，ステップＳ２１６、ステップＳ２２２のいずれかにおいて、チェック値の一致が得られなかった場合はエラーとして再生処理は終了する。

【０３６５】

ステップＳ２２４において全ブロック読み出しと判定されると、ステップＳ２２５に進み、コンテンツ（プログラム、データ）の実行、再生が開始される。

【０３６６】

以上が、フォーマットタイプ０におけるコンテンツデータの再生処理の態様である。

【０３６７】

次に、フォーマットタイプ１におけるコンテンツデータの再生処理について図４３を用いて説明する。上記したフォーマットタイプ０の再生処理と異なる点を中心に説明する。

【０３６８】

ステップＳ２０１～ステップＳ２１７までの処理は、上記したフォーマットタ

イプ０の再生処理と同様であるので説明は省略する。

【０３６９】

フォーマットタイプ１では、ステップＳ２３１において、暗号化パーツの復号が実行され、パーツＩＣＶが生成される。さらに、ステップＳ２３２において、ブロックＩＣＶｉ’が生成される。先に説明したように、フォーマット・タイプ１においては、ブロック内のパーツのうち少なくとも１つがチェック値ＩＣＶｉの対象データである場合は、そのブロックに関してコンテンツチェック値ＩＣＶｉが定義される。ブロックｉにおけるパーツｊのチェック値Ｐ－ＩＣＶｉｊは、パーツｊが暗号化されている場合、平文（復号文）全体を８バイト単位で排他論理和した値をコンテンツチェック値生成鍵Ｋｉｃｖｃで暗号化した値として生成される。また、パーツｊが暗号化されていない場合は、データ（平文）全体を８バイト単位で図３６に示す改竄チェック値生成関数（ＤＥＳ－ＣＢＣ－ＭＡＣ、コンテンツチェック値生成鍵Ｋｉｃｖｃを鍵とする）に入力して得た値として生成される。

【０３７０】

さらに、１つのブロックｉ内にチェツク対象であることを示す［ＩＣＶフラグ＝ｓｕｂｊｅｃｔ　ｏｆ　ＩＣＶ］であるパーツが１つのみ存在する場合は、上述の手法で生成したチェック値Ｐ－ＩＣＶｉｊをそのままブロックのチェック値ＩＣＶｉとし、また、１つのブロックｉ内にチェツク対象であることを示す［ＩＣＶフラグ＝ｓｕｂｊｅｃｔ　ｏｆ　ＩＣＶ］であるパーツが複数存在する場合は、複数のパーツチェック値Ｐ－ＩＣＶｉ，ｊをパーツ番号順に連結したデータを対象にしてデータ（平文）全体を８バイト単位で図３６に示す改竄チェック値生成関数（ＤＥＳ－ＣＢＣ－ＭＡＣ、コンテンツチェック値生成鍵Ｋｉｃｖｃを鍵とする）に入力して得た値として生成される。これは、先に図３７で説明した通りである。

【０３７１】

フォーマットタイプ１では、上述の手順で生成されたコンテンツチェック値の比較処理がステップＳ２２２で実行されることになる。以下のステップＳ２２３以下の処理はフォーマットタイプ０と同様であるので説明は省略する。

【０３７２】

次に、フォーマットタイプ２におけるコンテンツデータの再生処理について図４４を用いて説明する。上記したフォーマットタイプ０，１の再生処理と異なる点を中心に説明する。

【０３７３】

ステップＳ２０１～Ｓ２１０は、上記したフォーマットタイプ０，１の再生処理と同様であるので説明は省略する。

【０３７４】

フォーマットタイプ２においては、フォーマットタイプ０，１において実行されたステップＳ２１１～Ｓ２１６の処理が実行されない。また、フォーマットタイプ２においては、コンテンツチェック値を持たないため、フォーマットタイプ０，１において実行されたステップＳ２２２のコンテンツチェック値の検証も実行されない。

【０３７５】

フォーマットタイプ２のデータ再生処理においては、ステップＳ２１０のチェック値Ｂの検証ステップの後、ステップＳ２１７に進み、記録再生器３００の制御部３０１の制御によって、ブロックデータが読み出される。さらに、ステップＳ２４１において、記録再生器３００の暗号処理部３０６によるブロックデータに含まれるブロック鍵Ｋｂｌｃの復号処理が実行される。記録デバイス４００に格納されたブロック鍵Ｋｂｌｃは、図３４で示すようにコンテンツ鍵Ｋｃｏｎで暗号化されており、先のステップＳ２０７において復号したコンテンツ鍵Ｋｃｏｎを用いてブロック鍵Ｋｂｌｃの復号を行なう。

【０３７６】

次に、ステップＳ２４２において、ステップＳ２４１で復号されたブロック鍵Ｋｂｌｃを用いてブロックデータの復号処理が実行される。さらに、ステップＳ２４３において、コンテンツ（プログラム、データ）の実行、再生処理が実行される。ステップＳ２１７～ステップＳ２４３の処理が全ブロックについて繰り返し実行される。ステップＳ２４４において全ブロック読み出しと判定されると再生処理は終了する。

【０３７７】

このようにフォーマットタイプ２の処理は、総チェック値等のチェック値検証処理を省略しており、高速な復号処理の実行に適している構成であり、音楽データ等リアルタイム処理が要求されるデータ処理に適したフォーマットである。

【０３７８】

次にフォーマットタイプ３におけるコンテンツデータの再生処理について図４５を用いて説明する。上記したフォーマットタイプ０，１，２の再生処理と異なる点を中心に説明する。

【０３７９】

フォーマットタイプ３は、基本的にフォーマットタイプ２における処理と共通する部分が多いが、フォーマットタイプ３は図３５において説明したようにコンテンツ鍵を有しておらず、またブロック鍵Ｋｂｌｃが記録デバイスにおいては保存鍵Ｋｓｔｒで暗号化されて格納される点がフォーマットタイプ２と異なる。

【０３８０】

ステップＳ２０１～Ｓ２１０において、ステップＳ２５１、ステップＳ２５２、ステップＳ２５３、ステップＳ２５４の処理は、前述のフォーマットタイプ０，１，２における対応処理と異なりコンテンツ鍵を含まない処理として構成されている。

【０３８１】

ステップＳ２５１において、記録再生器３００の制御部３０１は、読み出したヘッダから記録デバイス固有の保存鍵Ｋｓｔｒで暗号化されたブロック情報鍵Ｋｂｉｔを取り出し、記録再生器３００の記録デバイスコントローラ３０３を介して記録デバイス４００に送信する。

【０３８２】

記録再生器３００から送信されてきたブロック情報鍵Ｋｂｉｔを受信した記録デバイス４００は、受信したデータを記録デバイス暗号処理部４０１の暗号／復号化部４０６に、記録デバイス暗号処理部４０１の内部メモリ４０５に保存してある記録デバイス固有の保存鍵Ｋｓｔｒで復号化処理させ、相互認証の際に共有

しておいたセッション鍵Ｋｓｅｓで再暗号化させる。この処理は、前述した（９）相互認証後の鍵交換処理の欄で詳しく述べた通りである。

【０３８３】

ステップＳ２５２では、記録再生器３００の制御部３０１は、記録再生器３００の記録デバイスコントローラ３０３を介し、記録デバイス４００からセッション鍵Ｋｓｅｓで再暗号化されたブロック情報鍵Ｋｂｉｔを受信する。

【０３８４】

次に、ステップＳ２５３において、記録再生器３００の制御部３０１は、受信したセッション鍵Ｋｓｅｓで再暗号化されたブロック情報鍵Ｋｂｉｔを記録再生器３００の記録再生器暗号処理部３０２に送信し、セッション鍵Ｋｓｅｓで再暗号化されたブロック情報鍵Ｋｂｉｔを受信した記録再生器３００の記録再生器暗号処理部３０２は、記録再生器暗号処理部３０２の暗号／復号化部３０８に、セッション鍵Ｋｓｅｓで暗号化されたブロック情報鍵Ｋｂｉｔを、相互認証の際に共有しておいたセッション鍵Ｋｓｅｓで復号化させる。

【０３８５】

さらに、ステップＳ２０８において、復号化したブロック情報鍵Ｋｂｉｔで、ステップＳ２０２で読み出しておいたブロック情報を復号化する。なお、記録再生器３００の記録再生器暗号処理部３０２は、復号化したブロック情報鍵Ｋｂｉｔおよびブロック情報ＢＩＴを、ステップＳ２０２で読み出したヘッダに含まれるブロック情報鍵Ｋｂｉｔおよびブロック情報ＢＩＴに置き換えて保持しておく。また、記録再生器３００の制御部３０１は、復号化されたブロック情報ＢＩＴを記録再生器３００の記録再生器暗号処理部３０２から読み出しておく。

【０３８６】

さらに、ステップＳ２５４において、記録再生器暗号処理部３０２の制御部３０６は、ブロック情報鍵Ｋｂｉｔおよびブロック情報（ＢＩＴ）から、チェック値Ｂ（ＩＣＶｂ’）を生成する。チェック値Ｂは、図２４に示すように、記録再生器暗号処理部３０２の内部メモリ３０７に保存されているチェック値Ｂ生成鍵Ｋｉｃｖｂを鍵とし、ブロック情報鍵Ｋｂｉｔおよびブロック情報（ＢＩＴ）からなる排他的論理和値をＤＥＳで暗号化して生成する。次に、ステップＳ２１０

において、チェック値Ｂとヘッダ（Header）内のＩＣＶｂを比較し、一致していた場合にはステップＳ２１１へ進む。

【０３８７】

フオーマットタイプ３では、さらに、ブロック鍵が記録デバイスでの格納時に保存鍵によって暗号化されるため、記録デバイス４００における保存鍵での復号処理、およびセッション鍵での暗号化処理、さらに、記録再生器３００でのセッション鍵での復号処理が必要となる。これらの一連の処理がステップＳ２５５、ステップＳ２５６で示した処理ステップである。

【０３８８】

ステップＳ２５５では、記録再生器３００の制御部３０１は、ステップＳ２１７で読み出したブロックから記録デバイス固有の保存鍵Ｋｓｔｒで暗号化されたブロック鍵Ｋｂｌｃを取り出し、記録再生器３００の記録デバイスコントローラ３０３を介して記録デバイス４００に送信する。

【０３８９】

記録再生器３００から送信されてきたブロック鍵Ｋｂｌｃを受信した記録デバイス４００は、受信したデータを記録デバイス暗号処理部４０１の暗号／復号化部４０６に、記録デバイス暗号処理部４０１の内部メモリ４０５に保存してある記録デバイス固有の保存鍵Ｋｓｔｒで復号化処理させ、相互認証の際に共有しておいたセッション鍵Ｋｓｅｓで再暗号化させる。この処理は、前述した「（９）相互認証後の鍵交換処理」の欄で詳しく述べた通りである。

【０３９０】

ステップＳ２５６では、記録再生器３００の制御部３０１は、記録再生器３００の記録デバイスコントローラ３０３を介し、記録デバイス４００からセッション鍵Ｋｓｅｓで再暗号化されたブロック鍵Ｋｂｌｃを受信する。

【０３９１】

次に、ステップＳ２５７において、記録再生器３００の暗号処理部３０６によるブロック鍵Ｋｂｌｃのセッション鍵Ｋｓｅｓを用いた復号処理が実行される。

【０３９２】

次に、ステップＳ２４２において、ステップＳ２５７で復号されたブロック鍵

Ｋｂｌｃを用いてブロックデータの復号処理が実行される。さらに、ステップＳ２４３において、コンテンツ（プログラム、データ）の実行、再生処理が実行される。ステップＳ２１７～ステップＳ２４３の処理が全ブロックについて繰り返し実行される。ステップＳ２４４において全ブロック読み出しと判定されると再生処理は終了する。

【０３９３】

以上の処理が、フォーマットタイプ３におけるコンテンツの再生処理である。総チェック値の検証処理が省略された点でフォーマットタイプ２と類似するが、ブロック鍵の鍵交換処理を含む点でフォーマットタイプ２に比較して、さらにセキュリテイ・レベルの高い処理構成となっている。

【０３９４】

（１１）コンテンツプロバイダにおけるチェック値（ＩＣＶ）生成処理態様

上述の実施例中において、各種のチェック値ＩＣＶについての検証処理が、コンテンツのダウンロード、または再生処理等の段階で実行されることを説明してきた。ここでは、これら各チェック値（ＩＣＶ）生成処理、検証処理の態様について説明する。

【０３９５】

まず、実施例で説明した各チェック値について、簡潔にまとめると、本発明のデータ処理装置において利用されるチェック値ＩＣＶには以下のものがある。

【０３９６】

チェック値Ａ，ＩＣＶａ：コンテンツデータ中の識別情報、取扱方針の改竄を検証するためのチェック値。

チェック値Ｂ，ＩＣＶｂ：ブロック情報鍵Ｋｂｉｔ、コンテンツ鍵Ｋｃｏｎ、ブロック情報の改竄を検証するためのチェック値。

コンテンツチェック値ＩＣＶｉ：コンテンツの各コンテンツブロックの改竄を検証するためのチェック値。

総チェック値ＩＣＶｔ：チェック値ＩＣＶａ、チェック値ＩＣＶｂ、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。

再生器固有チェック値ＩＣＶｄｅｖ：ローカリゼーションフラグが１にセット

されている場合、すなわち、コンテンツが記録再生器固有に利用可能であることを示している場合に、総チェック値ＩＣＶｔに置き換えられるチェック値であり、前述のチェック値Ａ：ＩＣＶａ、チェック値Ｂ：ＩＣＶｂ、さらにコンテンツのチェック対象となっている各ブロックに含まれるチェック値ＩＣＶｉ全体に対するチェック値として生成される。

フォーマットによっては、ＩＣＶｔ、ＩＣＶｄｅｖがチェックする対象に含まれるのは、各コンテンツブロックのチェック値ではなく、コンテンツそのものとなる場合もある。

【０３９７】

以上の各チェック値が本発明のデータ処理装置において用いられる。上記各チェック値の中で、チェック値Ａ、チェック値Ｂ、総チェック値、コンテンツチェック値は、例えば図３２～３５、および図６に示されるようにコンテンツデータを提供するコンテンツプロバイダ、あるいはコンテンツ管理者によって、それぞれの検証対象データに基づいてＩＣＶ値が生成され、コンテンツと共にデータ中に格納されて記録再生器３００の利用者に提供される。記録再生器の利用者、すなわちコンテンツ利用者は、このコンテンツを記録デバイスにダウンロードする際、または再生する際にそれぞれの検証対象データに基づいて検証用のＩＣＶを生成して、格納済みのＩＣＶとの比較を行なう。また、再生器固有チェック値ＩＣＶｄｅｖは、コンテンツが記録再生器固有に利用可能であることを示している場合に、総チェック値ＩＣＶｔに置き換えられて、記録デバイスに格納されるものである。

【０３９８】

チェック値の生成処理は、前述の実施例中では、主としてＤＥＳ－ＣＢＣによる生成処理構成を説明してきた。しかし、ＩＣＶの生成処理態様には、上述の方法に限らず様々な生成処理態様、さらに、様々な検証処理態様がある。特にコンテンツ提供者または管理者と、コンテンツ利用者との関係においては、以下に説明する各種のＩＣＶ生成および検証処理構成が可能である。

【０３９９】

図４６～図４８にチェック値ＩＣＶの生成者における生成処理と、検証者によ

る検証処理を説明する図を示す。

【０４００】

図４６は、上述の実施例中で説明したＤＥＳ－ＣＢＣによるＩＣＶの生成処理を、例えばコンテンツ提供者または管理者であるＩＣＶ生成者が行ない、生成したＩＣＶをコンテンツと共に記録再生器利用者、すなわち検証者に提供する構成である。この場合に記録再生器利用者、すなわち検証者が検証処理の際に必要となる鍵は、例えば図１８に示す内部メモリ３０７に格納された各チェック値生成鍵である。コンテンツ利用者である検証者（記録再生器利用者）は、内部メモリ３０７に格納されたチェック値生成鍵を使用して、検証対象のデータにＤＥＳ－ＣＢＣを適用してチェック値を生成して格納チェック値と比較処理を実行する。この場合、各チェック値生成鍵は、ＩＣＶの生成者と、検証者が秘密に共有する鍵として構成される。

【０４０１】

図４７は、コンテンツ提供者または管理者であるＩＣＶの生成者が公開鍵暗号系のデジタル署名によりＩＣＶを生成して、生成したＩＣＶをコンテンツと共にコンテンツ利用者、すなわち検証者に提供する。コンテンツ利用者、すなわち検証者は、ＩＣＶ生成者の公開鍵を保存し、この公開鍵を用いてＩＣＶの検証処理を実行する構成である。この場合、コンテンツ利用者（記録再生器利用者）、すなわち検証者の有するＩＣＶ生成者の公開鍵は秘密にする必要がなく、管理は容易となる。ＩＣＶの生成、管理が１つのエンティテイにおいて実行される場合等、ＩＣＶの生成、管理が高いセキュリティ管理レベルで行われている場合に適した態様である。

【０４０２】

図４８は、コンテンツ提供者または管理者であるＩＣＶの生成者が公開鍵暗号系のデジタル署名によりＩＣＶを生成して、生成したＩＣＶをコンテンツと共にコンテンツ利用者、すなわち検証者に提供し、さらに、検証者が検証に用いる公開鍵を公開鍵証明書（例えば図１４参照）に格納してコンテンツデータと共に記録再生器利用者、すなわち検証者に提供する。ＩＣＶの生成者が複数存在する場合には、各生成者は、公開鍵の正当性を証明するデータ（公開鍵証明書）を鍵管

理センタに作成してもらう。

【０４０３】

ＩＣＶの検証者であるコンテンツ利用者は、鍵管理センタの公開鍵を持ち、検証者は公開鍵証明書の検証を鍵管理センタの公開鍵によって実行し、正当性が確認されたら、その公開鍵証明書に格納されたＩＣＶの生成者の公開鍵を取り出す。さらに、取り出したＩＣＶの生成者の公開鍵を用いてＩＣＶの検証を実行する。

【０４０４】

この方法は、ＩＣＶの生成者が複数あり、それらの管理を実行するセンタによる管理の実行システムが確立している場合に有効な態様である。

【０４０５】

（１２）マスタ鍵に基づく暗号処理鍵生成構成

次に、本発明のデータ処理システムにおける特徴的な構成の１つである、マスタ鍵に基づく各種暗号処理用鍵の生成構成について説明する。

【０４０６】

先に図１８を用いて説明したように、本発明のデータ処理装置における記録再生器３００の内部メモリには、様々なマスタ鍵が格納され、これらの各マスタ鍵を用いて、例えば認証鍵Ｋａｋｅを生成（数３参照）したり、あるいは配送鍵Ｋｄｉｓを生成（数４参照）する構成となっている。

【０４０７】

従来、1対１のエンティテイ間、すなわちコンテンツプロバイダとコンテンツ利用者間、あるいは、上述の本発明のデータ処理装置における記録再生器３００と記録メディア４００との間において暗号通信、相互認証、ＭＡＣ生成、検証等を行なう際には、各エンティテイに共通な秘密情報、例えば鍵情報を保持させていた。また、１対多の関係、例えば１つのコンテンツプロバイダに対する多数のコンテンツ利用者、あるいは１つの記録再生器に対する多数の記録メディア等の関係においては、すべてのエンティテイ、すなわち多数のコンテンツ利用者、あるいは多数の記録メディアにおいて共有させた秘密情報、例えば鍵情報を格納保持させる構成とするか、あるいは、１つのコンテンツプロバイダが多数のコンテ

ンツ利用者各々の秘密情報（ｅｘ．鍵）を個別に管理し、これを各コンテンツ利用者に応じて使い分けていた。

【０４０８】

しかしながら、上記のような１対多の利用関係がある場合、すべてが共有する秘密情報（ｅｘ．鍵）を所有する構成においては、１箇所の秘密漏洩が発生すると同じ秘密情報（ｅｘ．鍵）を利用している者すべてに影響が及ぶという欠点がある。また、１つの管理者、例えばコンテンツプロバイダが多数のコンテンツ利用者各々の秘密情報（ｅｘ．鍵）を個別に管理し、これを各コンテンツ利用者に応じて使い分ける構成とすると、すべての利用者を識別し、かつその識別データに固有の秘密情報（ｅｘ．鍵）を対応づけたリストが必要となり、利用者の増大に伴うリストの保守管理の負担が増加するという欠点がある。

【０４０９】

本発明のデータ処理装置においては、このようなエンティテイ間における秘密情報の共有における従来の問題点をマスター鍵の保有、およびマスター鍵から各種の個別鍵を生成する構成により解決した。以下、この構成について説明する。

【０４１０】

本発明のデータ処理装置においては、記録デバイスやコンテンツを格納したメディア、または記録再生器間での各種の暗号処理、認証処理等において異なる個別の鍵が必要になる場合、その個別の鍵を、デバイスやメディアが固有に持つ識別子データ（ＩＤ）などの個別情報と記録再生器３００内であらかじめ決められた個別鍵生成方式を用いて生成する。この構成により万が一、生成された個別の鍵が特定された場合でもマスター鍵の漏洩を防止すれば、システム全体への被害を防ぐことが可能となる。またマスター鍵によって鍵を生成する構成により対応づけリストの管理も不要となる。

【０４１１】

具体的な構成例について、図を用いて説明する。まず、図４９に各種の鍵を記録再生器３００の有する各種のマスタ鍵を用いて生成する構成を説明する図を示す。図４９のメディア５００、通信手段６００からは、すでに説明した実施例と同様、コンテンツが入力される。コンテンツはコンテンツ鍵Ｋｃｏｎによって暗

号化され、またコンテンツ鍵Ｋｃｏｎは、配送鍵Ｋｄｉｓによって暗号化されている。

【０４１２】

例えば、記録再生器３００がメディア５００、通信手段６００からコンテンツを取り出して、記録デバイス４００にダウンロードしようとする場合、先の図２２、図３９～４１において説明したように、記録再生器３００は、コンテンツ鍵を暗号化している配送鍵Ｋｄｉｓを取得することが必要となる。このＫｄｉｓをメディア５００、通信手段６００から直接取得したり、あるいは予め記録再生器３００が取得して記録再生器３００内のメモリに格納しておくことも可能であるが、このような鍵の多数のユーザに対する配布構成は、先にも説明したようにシステム全体に影響を及ぼす漏洩の可能性がある。

【０４１３】

本発明のデータ処理システムでは、この配送鍵Ｋｄｉｓを図４９の下部に示すように、記録再生器３００のメモリに格納された配送鍵用マスター鍵ＭＫｄｉｓと、コンテンツＩＤに基づく処理、すなわちＫｄｉｓ＝ＤＥＳ（ＭＫｄｉｓ，コンテンツＩＤ）を適用して配送鍵Ｋｄｉｓを生成する構成としている。本構成によれば、メディア５００、通信手段６００からコンテンツを供給するコンテンツプロバイダとそのコンテンツ利用者である記録再生器３００間におけるコンテンツ配布構成において、コンテンツプロバイダが多数存在した場合であっても、個々の配送鍵Ｋｄｉｓをメディア、通信媒体等を介して流通させる必要もなく、また、各記録再生器３００に格納する必要もなく、セキュリティを高度に保つことが可能となる。

【０４１４】

次に、認証鍵Ｋａｋｅの生成について説明する。先に説明した図２２、図３９～４１の記録再生器３００から記録メディア４００に対するダウンロード処理、あるいは図２８，図４２～４５で説明した記録メディア４００に格納されたコンテンツを記録再生器３００において実行、再生する場合、記録再生器３００と記録メディア４００間における相互認証処理（図２０参照）が必要となる。

【０４１５】

図２０で説明したように、この認証処理において記録再生器３００は認証鍵Ｋａｋｅが必要となる。記録再生器３００は、認証鍵を例えば記録メディア４００から直接取得したり、あるいは予め記録再生器３００が取得して記録再生器３００内のメモリに格納しておくことも可能であるが、上述の配送鍵の構成と同様、このような鍵の多数のユーザに対する配布構成は、システム全体に影響を及ぼす漏洩の可能性がある。

【０４１６】

本発明のデータ処理システムでは、この認証鍵Ｋａｋｅを図４９の下部に示すように、記録再生器３００のメモリに格納された認証鍵用マスター鍵ＭＫａｋｅと、記録デバイス識別ＩＤ：ＩＤｍｅｍに基づく処理、すなわちＫａｋｅ＝ＤＥＳ（ＭＫａｋｅ，ＩＤｍｅｍ）によって認証鍵Ｋａｋｅを求める構成としている。

【０４１７】

さらに、図２２、図３９～４１の記録再生器３００から記録メディア４００に対するダウンロード処理、あるいは図２８，図４２～４５で説明した記録メディア４００に格納されたコンテンツを記録再生器３００において実行、再生する場合、記録再生器固有に利用可能なコンテンツである場合の記録再生器固有チェック値ＩＣＶｄｅｖの生成処理に必要となる記録再生器署名鍵Ｋｄｅｖについても上述の配送鍵、認証鍵と同様の構成とすることができる。上述の実施例中では、記録再生器署名鍵Ｋｄｅｖは内部メモリに格納する構成としていたが、記録再生器署名鍵用マスター鍵ＭＫｄｅｖをメモリに格納し、記録再生器署名鍵Ｋｄｅｖは内部メモリに格納せず、必要に応じて図４９の下部に示すように記録再生器識別子：ＩＤｄｅｖと記録再生器署名鍵用マスター鍵ＭＫｄｅｖに基づいて、Ｋｄｅｖ＝ＤＥＳ（ＭＫｄｅｖ，ＩＤｄｅｖ）によって記録再生器署名鍵Ｋｄｅｖを求める構成とすることで、記録再生器署名鍵Ｋｄｅｖを機器個別に持たせる必要がなくなるという利点が挙げられる。

【０４１８】

このように、本発明のデータ処理装置においては、プロバイダと記録再生器、あるいは記録再生器と記録デバイス間のような２つのエンテイテイ間における暗

号情報処理に関する手続きに必要な鍵等の情報をマスター鍵と各ＩＤから逐次的に生成する構成としたので、鍵情報が各エンテイテイから漏洩した場合でも、個別の鍵による被害の範囲はより限定され、また前述したような個別のエンテイテイごとの鍵リストの管理も不要となる。

【０４１９】

本構成に関する複数の処理例についてフローを示して説明する。図５０は、コンテンツ製作または管理者におけるマスター鍵を用いたコンテンツ等の暗号化処理と、ユーザデバイス、例えば上述の実施例における記録再生器３００におけるマスター鍵を用いた暗号化データの復号処理例である。

【０４２０】

コンテンツ製作または管理者におけるステップＳ５０１は、コンテンツに対する識別子（コンテンツＩＤ）を付与するステップである。ステップＳ５０２は、コンテンツ製作または管理者の有するマスター鍵とコンテンツＩＤとに基づいてコンテンツ等を暗号化する鍵を生成するステップである。これは例えば、配送鍵Ｋｄｉｓを生成する工程とすれば、前述のＫｄｉｓ＝ＤＥＳ（ＭＫｄｉｓ，コンテンツＩＤ）によって配送鍵Ｋｄｉｓを生成する。次に、ステップＳ５０３は、コンテンツの一部、または全部を鍵（例えば配送鍵Ｋｄｉｓ）によって暗号化するステップである。コンテンツ製作者は、このようなステップを経て暗号化処理を行なったコンテンツをＤＶＤ等のメディア、通信手段等を介して配信する。

【０４２１】

一方、例えば記録再生器３００等のユーザデバイス側では、ステップＳ５０４において、メディア、通信手段等を介して受領したコンテンツデータ中からコンテンツＩＤを読み出す。次に、ステップＳ５０５において、読み出したコンテンツＩＤと所有するマスター鍵に基づいて暗号化コンテンツの復号に適用する鍵を生成する。この生成処理は、配送鍵Ｋｄｉｓを得るものである場合は、例えば配送鍵Ｋｄｉｓ＝ＤＥＳ（ＭＫｄｉｓ，コンテンツＩＤ）となる。ステップＳ５０６で、この鍵を用いてコンテンツを復号し、ステップＳ５０７で復号コンテンツの利用、すなわち再生またはプログラムを実行する。

【０４２２】

この例においては、図５０下段に示すように、コンテンツ製作または管理者と、ユーザデバイスの双方がマスター鍵（例えば配送鍵生成用マスター鍵ＭＫｄｉｓ）を有し、コンテンツの暗号化、復号に必要な配送鍵を逐次的にそれぞれの所有するマスター鍵と各ＩＤ（コンテンツＩＤ）に基づいて生成する。

【０４２３】

このシステムでは、万が一配送鍵が第三者に漏洩した場合、そのコンテンツの復号が第三者において可能となるが、コンテンツＩＤの異なる他のコンテンツの復号は防止することが可能であるため、１つのコンテンツ鍵の漏洩がシステム全体に及ぼす影響を最小限にすることができるという効果がある。また、ユーザデバイス側、すなわち記録再生器において、コンテンツ毎の鍵の対応付けリストを保持する必要がないという効果もある。

【０４２４】

次に図５１を用いて、コンテンツ製作または管理者が複数のマスター鍵を所有して、コンテンツの配信対象に応じた処理を実行する例について説明する。

【０４２５】

コンテンツ製作または管理者におけるステップＳ５１１は、コンテンツに対する識別子（コンテンツＩＤ）を付与するステップである。ステップＳ５１２は、コンテンツ製作または管理者の有する複数のマスター鍵（例えば複数の配送鍵生成用マスター鍵ＭＫｄｉｓ）から１つのマスター鍵を選択するステップである。この選択処理は図５２を用いてさらに説明するが、コンテンツの利用者の国ごと、機種ごと、あるいは機種のバージョンごとなどに対応付けて予め適用するマスター鍵を設定しておき、その設定に従って実行するものである。

【０４２６】

次に、ステップＳ５１３では、ステップＳ５１２で選択したマスター鍵と、ステップＳ５１１で決定したコンテンツＩＤとに基づいて暗号化用の鍵を生成する。これは例えば、配送鍵Ｋｄｉｓｉを生成する工程とすれば、Ｋｄｉｓｉ＝ＤＥＳ（ＭＫｄｉｓｉ，コンテンツＩＤ）によって生成する。次に、ステップＳ５１４はコンテンツの一部、または全部を鍵（例えば配送鍵Ｋｄｉｓｉ）によって暗号化するステップである。コンテンツ製作者は、ステップＳ５１５において、コ

ンテンツＩＤと、使用したマスター鍵識別情報と、暗号化コンテンツを１つの配布単位として暗号化処理を行なったコンテンツをＤＶＤ等のメディア、通信手段等を介して配信する。

【０４２７】

一方、例えば記録再生器３００等のユーザデバイス側では、ステップＳ５１６において、ＤＶＤ等のメディア、通信手段等を介して配信されたコンテンツデータ中のマスター鍵識別情報に対応するマスター鍵を自己が所有するか否かについて判定する。コンテンツデータ中のマスター鍵識別情報に対応するマスター鍵を持たない場合は、その配布コンテンツは、そのユーザデバイスにおいては利用できないものであり、処理は終了する。

【０４２８】

配信されたコンテンツデータ中のマスター鍵識別情報に対応するマスター鍵を自己が所有する場合は、ステップＳ５１７において、メディア、通信手段等を介して受領したコンテンツデータ中からコンテンツＩＤを読み出す。次に、ステップＳ５１８において、読み出したコンテンツＩＤと所有するマスター鍵に基づいて暗号化コンテンツの復号に適用する鍵を生成する。この生成処理は、配送鍵Ｋｄｉｓｉを得るものである場合は、例えば配送鍵Ｋｄｉｓｉ＝ＤＥＳ（ＭＫｄｉｓｉ，コンテンツＩＤ）となる。ステップＳ５１９で、この鍵を用いてコンテンツを復号し、ステップＳ５２０で復号コンテンツの利用、すなわち再生またはプログラムを実行する。

【０４２９】

この例においては、図５１下段に示すように、コンテンツ製作または管理者は、複数のマスター鍵、例えば複数の配送鍵生成用マスター鍵ＭＫｄｉｓ１～ｎからなるマスター鍵セットを有する。一方、ユーザデバイスには１つのマスター鍵例えば１つの配送鍵生成用マスター鍵ＫＫｄｉｓｉを有し、コンテンツ製作または管理者がＭＫｄｉｓｉを用いて暗号化処理している場合のみ、ユーザデバイスは、そのコンテンツを復号して利用することができる。

【０４３０】

この図５１のフローに示す態様の具体例として、国毎に異なるマスター鍵を適

用した例を図５２に示す。コンテンツプロバイダは、マスター鍵ＭＫ１～ｎを有し、ＭＫ１は日本向けのユーザデバイスに配信するコンテンツの暗号化処理を実行する鍵生成に用いる。例えば、コンテンツＩＤとＭＫ１から暗号化鍵Ｋ１を生成してＫ１によってコンテンツを暗号化する。また、ＭＫ２はＵＳ向けのユーザデバイスに配信するコンテンツの暗号化処理を実行する鍵生成に用い、ＭＫ３はＥＵ（ヨーロッパ）向けのユーザデバイスに配信するコンテンツの暗号化処理を実行する鍵生成に用いるよう設定している。

【０４３１】

一方、日本向けユーザデバイス、具体的には日本で販売されるＰＣまたはゲーム機器等の記録再生器には、マスター鍵ＭＫ１がその内部メモリに格納され、ＵＳ向けユーザデバイスには、マスター鍵ＭＫ２がその内部メモリに格納され、ＥＵ向けユーザデバイスには、マスター鍵ＭＫ３がその内部メモリに格納されている。

【０４３２】

このような構成において、コンテンツプロバイダは、コンテンツを利用可能なユーザデバイスに応じて、マスター鍵ＭＫ１～ｎから、マスター鍵を選択的に使用してユーザデバイスに配信するコンテンツの暗号化処理を実行する。例えばコンテンツを日本向けのユーザデバイスのみ利用可能とするためには、マスター鍵ＭＫ１を用いて生成された鍵Ｋ１によってコンテンツを暗号化する。この暗号化コンテンツは、日本向けユーザデバイスに格納されたマスター鍵ＭＫ１を用いて復号可能、すなわち復号鍵を生成可能であるが、他のＵＳ、またはＥＵ向けのユーザデバイスに格納されたマスター鍵ＭＫ２，ＭＫ３からは鍵Ｋ１を得ることができないので、暗号化コンテンツの復号は不可能となる。

【０４３３】

このように、コンテンツプロバイダが複数のマスター鍵を選択的に使用することにより、様々なコンテンツの利用制限を設定することができる。図５２では、ユーザデバイスの国別にマスター鍵を区別する例を示したが、前述のように、ユーザデバイスの機種に応じて、あるいはバージョンに応じてマスター鍵を切り換える等、様々な利用形態が可能である。

【０４３４】

次に、図５３にメデイア固有の識別子、すなわちメディアＩＤとマスター鍵を組み合わせた処理例を示す。ここで。メディアとは例えばＤＶＤ、ＣＤ等のコンテンツを格納したメディアである。メディアＩＤは、１つ１つのメディアごとに固有としてもよいし、たとえば、映画などのコンテンツのタイトルごとに固有としてもよいし、メディアの製造ロットごとに固有としてもよい。このようにメディアＩＤの割り当て方法としては様々な方法を用いることができる。

【０４３５】

メデイア製作または管理者におけるステップＳ５２１は、メディアに対する識別子（メディアＩＤ）を決定するステップである。ステップＳ５２２は、メディア製作または管理者の有するマスター鍵とメディアＩＤとに基づいてメディア内の格納コンテンツ等を暗号化する鍵を生成するステップである。これは例えば、配送鍵Ｋｄｉｓを生成する工程とすれば、前述のＫｄｉｓ＝ＤＥＳ（ＭＫｄｉｓ，メディアＩＤ）によって配送鍵Ｋｄｉｓを生成する。次に、ステップＳ５２３は、メディア格納コンテンツの一部、または全部を鍵（例えば配送鍵Ｋｄｉｓ）によって暗号化するステップである。メディア製作者は、このようなステップを経て暗号化処理を行なったコンテンツ格納メディアを供給する。

【０４３６】

一方、例えば記録再生器３００等のユーザデバイス側では、ステップＳ５２４において、供給されたメディアからメディアＩＤを読み出す。次に、ステップＳ５２５において、読み出したメディアＩＤと所有するマスター鍵に基づいて暗号化コンテンツの復号に適用する鍵を生成する。この生成処理は、配送鍵Ｋｄｉｓを得るものである場合は、例えば配送鍵Ｋｄｉｓ＝ＤＥＳ（ＭＫｄｉｓ，メディアＩＤ）となる。ステップＳ５２６で、この鍵を用いてコンテンツを復号し、ステップＳ５２７で復号コンテンツの利用、すなわち再生またはプログラムを実行する。

【０４３７】

この例においては、図５３下段に示すように、メディア製作または管理者と、ユーザデバイスの双方がマスター鍵（例えば配送鍵生成用マスター鍵ＭＫｄｉｓ

）を有し、コンテンツの暗号化、復号に必要な配送鍵を逐次的にそれぞれの所有するマスター鍵と各ＩＤ（メディアＩＤ）に基づいて生成する。

【０４３８】

このシステムでは、万が一メディア鍵が第三者に漏洩した場合、そのメディア内のコンテンツの復号が第三者において可能となるが、メディアＩＤの異なる他のメディアに格納されたコンテンツの復号は防止することが可能であるため、１つのメディア鍵の漏洩がシステム全体に及ぼす影響を最小限にすることができるという効果がある。また、ユーザデバイス側、すなわち記録再生器において、メディア毎の鍵の対応付けリストを保持する必要がないという効果もある。また、１つのメディア鍵で暗号化されるコンテンツサイズは、そのメデイア内に格納可能な容量に制限されるため、暗号文攻撃のために必要な情報量に達する可能性は少なく、暗号解読の可能性を低減させることができる。

【０４３９】

次に、図５４に記録再生器固有の識別子、すなわち記録再生器ＩＤとマスター鍵を組み合わせた処理例を示す。

【０４４０】

記録再生器利用者におけるステップＳ５３１は、記録再生器の例えば内部メモリに格納されたマスター鍵と記録再生器ＩＤとに基づいてコンテンツ等を暗号化する鍵を生成するステップである。これは例えば、コンテンツ鍵Ｋｃｏｎを生成する工程とすれば、Ｋｃｏｎ＝ＤＥＳ（ＭＫｃｏｎ，記録再生器ＩＤ）によってコンテンツ鍵Ｋｃｏｎを生成する。次に、ステップＳ５３２は、格納するコンテンツの一部、または全部を鍵（例えば配送鍵Ｋｃｏｎ）によって暗号化するステップである。ステップＳ５３３は、暗号化コンテンツを例えばハードディスク等の記録デバイスに格納する。

【０４４１】

一方、記録再生器を管理するシステム管理者側では、コンテンツを格納した記録再生器利用者から格納データの復旧を依頼されると、ステップＳ５３４において、記録再生器から、記録再生器ＩＤを読み出す。次に、ステップＳ５３５において、読み出した記録再生器ＩＤと所有するマスター鍵に基づいて暗号化コンテ

ンツの復号に適用する鍵を生成する。この生成処理は、コンテンツ鍵Ｋｃｏｎを得るものである場合は、例えばコンテンツ鍵Ｋｃｏｎ＝ＤＥＳ（ＭＫｃｏｎ，記録再生器ＩＤ）となる。ステップＳ５３６で、この鍵を用いてコンテンツを復号する。

【０４４２】

この例においては、図５４下段に示すように、記録再生器利用者と、システム管理者の双方がマスター鍵（例えばコンテンツ鍵生成用マスター鍵ＭＫｃｏｎ）を有し、コンテンツの暗号化、復号に必要な配送鍵を逐次的にそれぞれの所有するマスター鍵と各ＩＤ（記録再生器ＩＤ）に基づいて生成する。

【０４４３】

このシステムでは、万が一コンテンツ鍵が第三者に漏洩した場合、そのコンテンツの復号が第三者において可能となるが、記録再生器ＩＤの異なる他の記録再生器用に暗号化されたコンテンツの復号は防止することが可能であるため、１つのコンテンツ鍵の漏洩がシステム全体に及ぼす影響を最小限にすることができるという効果がある。また、システム管理側、ユーザデバイス側両者において、コンテンツ毎の鍵の対応付けリストを保持する必要がないという効果もある。

【０４４４】

図５５は、スレーブデバイス、例えばメモリカード等の記録デバイスと、ホストデバイス、例えば記録再生器間における相互認証処理に用いる認証鍵をマスター鍵に基づいて生成する構成である。先に説明した認証処理（図２０参照）では、スレーブデバイスの内部メモリに認証鍵を予め格納した構成としてあるが、これを図５５に示すように認証処理時にマスター鍵に基づいて生成する構成とすることができる。

【０４４５】

例えば記録デバイスであるスレーブデバイスは、認証処理開始前の初期化処理として、ステップＳ５４１において、記録デバイスであるスレーブデバイスの内部メモリに格納したマスター鍵とスレーブデバイスＩＤとに基づいて相互認証処理に用いる認証鍵Ｋａｋｅを生成する。これは例えば、Ｋａｋｅ＝ＤＥＳ（ＭＫａｋｅ，スレーブデバイスＩＤ）によって生成する。次に、ステップＳ５４２に

おいて、生成した認証鍵をメモリに格納する。

【０４４６】

一方、例えば記録再生器等のホストデバイス側では、ステップＳ５４３において、装着された記録デバイス、すなわちスレーブデバイスから、通信手段を介してスレーブデバイスＩＤを読み出す。次に、ステップＳ５４４において、読み出したスレーブデバイスＩＤと所有する認証鍵生成用マスター鍵に基づいて相互認証処理に適用する認証鍵を生成する。この生成処理は、例えば認証鍵Ｋａｋｅ＝ＤＥＳ（ＭＫａｋｅ，スレーブデバイスＩＤ）となる。ステップＳ５４５で、この認証鍵を用いて認証処理を実行する。

【０４４７】

この例においては、図５５下段に示すように、スレーブデバイスと、マスターデバイスの双方がマスター鍵、すなわち認証鍵生成用マスター鍵ＭＫａｋｅを有し、相互認証処理に必要な認証鍵を逐次的にそれぞれの所有するマスター鍵とスレーブデバイスＩＤに基づいて生成する。

【０４４８】

このシステムでは、万が一認証鍵が第三者に漏洩した場合、その認証鍵は、そのスレーブデバイスのみに有効であるため、他のスレーブデバイスとの関係においては、認証が成立しないことになり、鍵の漏洩によって発生する影響を最小限にすることができるという効果がある。

【０４４９】

このように、本発明のデータ処理装置においては、コンテンツプロバイダと記録再生器、あるいは記録再生器と記録デバイス間のような２つのエンテイテイ間における暗号情報処理に関する手続きに必要な鍵等の情報をマスター鍵と各ＩＤから逐次的に生成する構成とした。従って、鍵情報が各エンテイテイから漏洩した場合でも、個別の鍵による被害の範囲はより限定され、また前述したような個別のエンテイテイごとの鍵リストの管理も不要となる。

【０４５０】

（１３）暗号処理における暗号強度の制御

上述した実施例において、記録再生器３００と記録デバイス４００間での暗号

処理は、説明を理解しやすくするため、主として、先に図７を用いて説明したシングルＤＥＳ構成による暗号処理を用いた例について説明してきた。しかしながら、本発明のデータ処理装置において適用される暗号化処理方式は上述したシングルＤＥＳ方式に何ら限定されるものではなく、必要なセキュリティ状態に応じた暗号化方式を採用することが可能である。

【０４５１】

例えば先に説明した図８～図１０の構成のようなトリプルＤＥＳ方式を適用してもよい。例えば図３に示す記録再生器３００の暗号処理部３０２と、記録デバイス４００の暗号処理部４０１の双方において、トリプルＤＥＳ方式を実行可能な構成とし、図８～図１０で説明したトリプルＤＥＳ方式による暗号処理に対応する処理を実行する構成が可能である。

【０４５２】

しかしながら、コンテンツの提供者は、コンテンツに応じて処理速度を優先してコンテンツ鍵Ｋｃｏｎをシングルｄｅｓ方式による６４ビット鍵構成とする場合もあり、また、セキュリティを優先してコンテンツ鍵Ｋｃｏｎをトリプルｄｅｓ方式による１２８ビット、または１９２ビット鍵構成とする場合もある。従って、記録再生器３００の暗号処理部３０２と、記録デバイス４００の暗号処理部４０１の構成をトリプルＤＥＳ方式、シングルＤＥＳ方式いずれか一方の方式にのみ対応可能な構成とすることは好ましくない。従って、記録再生器３００の暗号処理部３０２と、記録デバイス４００の暗号処理部４０１は、シングルＤＥＳ、トリプルＤＥＳいずれの方式にも対応可能とする構成が望ましい。

【０４５３】

しかしながら、記録再生器３００の暗号処理部３０２と、記録デバイス４００の暗号処理部４０１の暗号処理構成をシングルＤＥＳ方式、トリプルＤＥＳ方式の双方を実行可能な構成とするためには、それぞれの別の回路、ロジックを構成しなければならない。例えば、記録デバイス４００においてトリプルＤＥＳに対応する処理を実行するためには、先の図２９に示すコマンドレジスタにトリプルＤＥＳの命令セットを新たに格納することが必要となる。これは記録デバイス４００に構成する処理部の複雑化を招くこととなる。

【０４５４】

そこで、本発明のデータ処理装置は、記録デバイス４００側の暗号処理部４０１の有するロジックをシングルＤＥＳ構成として、かつトリプルＤＥＳ暗号化処理に対応した処理が実行可能で、トリプルＤＥＳ方式による暗号化データ(鍵、コンテンツ等)を記録デバイスの外部メモリ４０２に格納することを可能とした構成を提案する。

【０４５５】

例えば図３２に示すデータフォーマットタイプ０の例において、記録再生器３００から記録デバイス４００に対してコンテンツデータのダウンロードを実行する際、先に説明したフォーマットタイプ０のダウンロードのフローを示す図３９のステップＳ１０１で認証処理を実行し、ここでセッション鍵Ｋｓｅｓを生成する。さらに、ステップＳ１１７において、記録再生器３００側の暗号処理部３０２においてセッション鍵Ｋｓｅｓによるコンテンツ鍵Ｋｃｏｎの暗号化処理が実行され、この暗号化鍵が記録デバイス４００に通信手段を介して転送され、ステップＳ１１８において、この暗号化鍵を受信した記録デバイス４００の暗号処理部４０３がセッション鍵Ｋｓｅｓによるコンテンツ鍵Ｋｃｏｎの復号処理を実行し、さらに、保存鍵Ｋｓｔｒによるコンテンツ鍵Ｋｃｏｎの暗号化処理を実行して、これを記録再生器３００の暗号処理部３０２に送信し、その後、記録再生器３００がデータフォーマットを形成（ステップＳ１２１）してフォーマット化されたデータを記録デバイス４００に送信し、記録デバイス４００が受信したデータを外部メモリ４０２に格納する処理を行なっている。

【０４５６】

上記処理においてステップＳ１１７，Ｓ１１８間において実行される記録デバイス４００の暗号処理部４０１での暗号処理をシングルＤＥＳ、またはトリプルＤＥＳいずれかの方式を選択的に実行可能な構成とすれば、コンテンツ提供業者がトリプルＤＥＳにしたがったコンテンツ鍵Ｋｃｏｎを用いたコンテンツデータを提供する場合も、またシングルＤＥＳにしたがったコンテンツ鍵Ｋｃｏｎを用いたコンテンツデータを提供する場合も、いずれの場合にも対応可能となる。

【０４５７】

図５６に本発明のデータ処理装置における記録再生器３００の暗号処理部３０２と、記録デバイス４００の暗号処理部４０１との双方を用いてトリプルＤＥＳ方式に従った暗号処理方法を実行する構成を説明するフローを示す。図５６では、一例として記録再生器３００からコンテンツデータを記録デバイス４００にダウンロードする際に実行される保存鍵Ｋｓｔｒを用いたコンテンツ鍵Ｋｃｏｎの暗号化処理例であり、コンテンツ鍵Ｋｃｏｎがトリプルｄｅｓ方式による鍵である場合の例を示している。なお、ここでは、コンテンツ鍵Ｋｃｏｎを代表して、その処理例を示すが、他の鍵、またはコンテンツ等、その他のデータについても同様の処理が可能である。

【０４５８】

トリプルＤＥＳ方式においては、先の図８～１０において説明したように、シングルＤＥＳでは６４ビット鍵、トリプルＤＥＳ方式による場合は、１２８ビット、または１９２ビット鍵構成として、２つ、または３つの鍵が用いられる処理である。これら３つのコンテンツ鍵をそれぞれＫｃｏｎ１，Ｋｃｏｎ２，（Ｋｃｏｎ３）とする。Ｋｃｏｎ３は用いられない場合もあるので、かっこで示している。

【０４５９】

図５６の処理について説明する。ステップＳ３０１は記録再生器３００と、記録デバイス４００間での相互認証処理ステップである。この相互認証処理ステップは、先に説明した図２０の処理によって実行される。なお、この認証処理の際、セッション鍵Ｋｓｅｓが生成される。

【０４６０】

ステップＳ３０１の認証処理が終了すると、ステップＳ３０２において、各チェック値、チェック値Ａ，チェック値Ｂ、コンテンツチェック値、総チェック値、各ＩＣＶの照合処理が実行される。

【０４６１】

これらのチェック値（ＩＣＶ）照合処理が終了し、データ改竄がないと判定されると、ステップＳ３０３に進み、記録再生器３００において、記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部

３０８を使って、先に取り出したまたは生成した配送鍵Ｋｄｉｓを用いて、受信したメディア５００、または、通信部３０５を介して通信手段６００から受信したデータのヘッダ部に格納されたコンテンツ鍵Ｋｃｏｎの復号化処理を行う。この場合のコンテンツ鍵は、トリプルＤＥＳ方式による鍵であり、コンテンツ鍵Ｋｃｏｎ１，Ｋｃｏｎ２，（Ｋｃｏｎ３）である。

【０４６２】

次に、ステップＳ３０４において、記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８において、ステップＳ３０３で復号化したコンテンツ鍵Ｋｃｏｎ１，Ｋｃｏｎ２，（Ｋｃｏｎ３）の中のコンテンツ鍵Ｋｃｏｎ１のみを相互認証の際に共有しておいたセッション鍵Ｋｓｅｓで暗号化する。

【０４６３】

記録再生器３００の制御部３０１は、セッション鍵Ｋｓｅｓで暗号化されたコンテンツ鍵Ｋｃｏｎ１を含むデータを記録再生器３００の記録再生器暗号処理部３０２から読み出し、これらのデータを記録再生器３００の記録デバイスコントローラ３０３を介して記録デバイス４００に送信する。

【０４６４】

次に、ステップＳ３０５において、記録再生器３００から送信されてきたコンテンツ鍵Ｋｃｏｎ１を受信した記録デバイス４００は、受信したコンテンツ鍵Ｋｃｏｎ１を記録デバイス暗号処理部４０１の暗号／復号化部４０６に、相互認証の際に共有しておいたセッション鍵Ｋｓｅｓで復号化する。さらに、ステップＳ３０６において、記録デバイス暗号処理部４０１の内部メモリ４０５に保存してある記録デバイス固有の保存鍵Ｋｓｔｒで再暗号化させて、通信部４０４を介して記録再生器３００に送信する。

【０４６５】

次に、ステップＳ３０７において、記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８において、ステップＳ３０３で復号化したコンテンツ鍵Ｋｃｏｎ１，Ｋｃｏｎ２，（Ｋｃｏｎ３）の中のコンテンツ鍵Ｋｃｏｎ２のみを相互認証の際に共有しておいたセッション鍵

Ｋｓｅｓで暗号化する。

【０４６６】

記録再生器３００の制御部３０１は、セッション鍵Ｋｓｅｓで暗号化されたコンテンツ鍵Ｋｃｏｎ２を含むデータを記録再生器３００の記録再生器暗号処理部３０２から読み出し、これらのデータを記録再生器３００の記録デバイスコントローラ３０３を介して記録デバイス４００に送信する。

【０４６７】

次に、ステップＳ３０８において、記録再生器３００から送信されてきたコンテンツ鍵Ｋｃｏｎ２を受信した記録デバイス４００は、受信したコンテンツ鍵Ｋｃｏｎ２を記録デバイス暗号処理部４０１の暗号／復号化部４０６に、相互認証の際に共有しておいたセッション鍵Ｋｓｅｓで復号化する。さらに、ステップＳ３０９において、記録デバイス暗号処理部４０１の内部メモリ４０５に保存してある記録デバイス固有の保存鍵Ｋｓｔｒで再暗号化させて、通信部４０４を介して記録再生器３００に送信する。

【０４６８】

次に、ステップＳ３１０において、記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８において、ステップＳ３０３で復号化したコンテンツ鍵Ｋｃｏｎ１，Ｋｃｏｎ２，（Ｋｃｏｎ３）の中のコンテンツ鍵Ｋｃｏｎ３のみを相互認証の際に共有しておいたセッション鍵Ｋｓｅｓで暗号化する。

【０４６９】

記録再生器３００の制御部３０１は、セッション鍵Ｋｓｅｓで暗号化されたコンテンツ鍵Ｋｃｏｎ３を含むデータを記録再生器３００の記録再生器暗号処理部３０２から読み出し、これらのデータを記録再生器３００の記録デバイスコントローラ３０３を介して記録デバイス４００に送信する。

【０４７０】

次に、ステップＳ３１１において、記録再生器３００から送信されてきたコンテンツ鍵Ｋｃｏｎ３を受信した記録デバイス４００は、受信したコンテンツ鍵Ｋｃｏｎ３を記録デバイス暗号処理部４０１の暗号／復号化部４０６に、相互認証

の際に共有しておいたセッション鍵Ｋｓｅｓで復号化する。さらに、ステップＳ３１２において、記録デバイス暗号処理部４０１の内部メモリ４０５に保存してある記録デバイス固有の保存鍵Ｋｓｔｒで再暗号化させて、通信部４０４を介して記録再生器３００に送信する。

【０４７１】

次にステップＳ３１３において、記録再生器の暗号処理部は、図３２～３５で説明した各種のデータフォーマットを形成して、記録デバイス４００に送信する。

【０４７２】

最後にステップＳ３１４において、記録デバイス４００は、フォーマット形成が終了した受信データを外部メモリ４０２に格納する。このフオーマットデータには、保存鍵Ｋｓｔｒで暗号化されたコンテンツ鍵Ｋｃｏｎ１，Ｋｃｏｎ２，（Ｋｃｏｎ３）を含んでいる。

【０４７３】

このような処理を実行することにより、記録デバイス４００に格納するコンテンツ鍵をトリプルＤＥＳ方式の暗号方式による鍵として格納することが可能となる。なお、コンテンツ鍵がＫｃｏｎ１，Ｋｃｏｎ２の２つの鍵である場合は、ステップＳ３１０～Ｓ３１２の処理は省略される。

【０４７４】

このように、記録デバイス４００は、同じ態様の処理、すなわちステップＳ３０５，Ｓ３０６の処理ステップを複数回、その対象を変更するのみで繰り返し実行することにより、トリプルＤＥＳの適用された鍵をメモリに格納可能となる。コンテンツ鍵ＫｃｏｎがシングルＤＥＳの適用鍵である場合は、ステップＳ３０５，Ｓ３０６を実行して、ステップＳ３１３のフォーマット化処理を実行してメモリに格納すればよい。このような構成は、ステップＳ３０５，Ｓ３０６の処理を実行するコマンドを先に説明した図２９のコマンドレジスタに格納し、この処理をコンテンツ鍵の態様、すなわちトリプルＤＥＳ方式か、シングルＤＥＳ方式かによって、適宜１回～３回実行する構成とすればよい。従って、記録デバイス４００の処理ロジック中にトリプルＤＥＳの処理方式を含ませることなく、トリ

プルＤＥＳ方式、シングルＤＥＳ方式、の双方の処理が可能となる。なお、暗号化方式については、コンテンツデータのヘッダ部内の取扱方針に記録し、これを参照することで判定することが可能である。

【０４７５】

（１４）コンテンツデータにおける取扱方針中の起動優先順位に基づくプログラム起動処理

先に説明した図４～６のコンテンツデータ構成から理解されるように、本発明のデータ処理装置において利用されるコンテンツデータのヘッダ部に格納された取扱方針には、コンテンツタイプ、起動優先順位情報が含まれる。本発明のデータ処理装置における記録再生器３００は、記録デバイス４００、あるいは、ＤＶＤ、ＣＤ、ハードディスク、さらにはゲームカートリッジ等の各種記録媒体に記録されたアクセス可能なコンテンツデータが複数存在する場合、これらコンテンツの起動順位を起動優先順位情報に従って決定する。

【０４７６】

記録再生器３００は、各記録デバイスＤＶＤ装置、ＣＤドライブ装置、ハードデイスクドライブ装置等各種記録デバイスとの認証処理を実行後、コンテンツデータ中の優先順位情報に従って、最も優先順位の高いコンテンツデータ中のプログラムを優先して実行する。以下、この「コンテンツデータにおける取扱方針中の起動優先順位に基づくプログラム起動処理」について説明する。

【０４７７】

上述した本発明のデータ処理装置実施例の説明においては、記録再生器３００が１つの記録デバイス４００からコンテンツデータを再生、実行する場合の処理を中心として説明した。しかし、一般に記録再生器３００は、図２に示すように記録デバイス４００の他に、読み取り部３０４を介してＤＶＤ、ＣＤ、ハードディスク、さらに、ＰＩＯ１１１、ＳＩＯ１１２を介して接続されるメモリカード、ゲームカートリッジ等、各種記録媒体にアクセス可能な構成を有する。なお、図２では、図の複雑化を避けるため読み取り部３０４を１つのみ記載しているが、記録再生器３００は、異なる記憶媒体、例えばＤＶＤ、ＣＤ、フロッピーディスク、ハードディスクを並列に装着可能である。

【０４７８】

記録再生器３００は、複数の記憶媒体にアクセス可能であり、それぞれの記憶媒体にはそれぞれコンテンツデータが格納されている。例えばＣＤ等外部のコンテンツプロバイダが供給するコンテンツデータは、前述の図４のデータ構成でメディアに格納され、これらのメディアまたは、通信手段を介してダウンロードした場合には、図２６、図２７のコンテンツデータ構成でメモリカード等の各記憶媒体に格納されている。さらに、具体的には、コンテンツデータのフォーマットタイプに応じて図３２～３５に示すようにメディア上、記録デバイス上でそれぞれ異なるフォーマットで格納される。しかし、いずれの場合にもコンテンツデータのヘッダ中の取扱方針にはコンテンツタイプ、起動優先順位情報が含まれる。

【０４７９】

これら、複数のコンテンツデータに対するアクセスが可能な場合の記録再生器のコンテンツ起動処理をフローに従って説明する。

【０４８０】

図５７は、起動可能コンテンツが複数ある場合の処理例（１）を示す処理フローである。ステップＳ６１１は、記録再生器３００がアクセス可能な記録デバイスの認証処理を実行するステップである。アクセス可能な記録デバイスには、メモリカード、ＤＶＤ装置、ＣＤドライブ、ハードディスク装置、さらに、例えばＰＩＯ１１１、ＳＩＯ１１２を介して接続されるゲームカートリッジ等が含まれる。認証処理は、図２で示す制御部３０１の制御のもとに各記録デバイスに対して例えば先に図２０で説明した手順に従って実行される。

【０４８１】

次に、ステップＳ６１２おいて、認証に成功した記録デバイス内のメモリに格納されたコンテンツデータから起動可能なプログラムを検出する。これは、具体的には、コンテンツデータの取扱方針に含まれるコンテンツタイプがプログラムであるものを抽出する処理として実行される。

【０４８２】

次に、ステップＳ６１３において、ステップＳ６１２で抽出された起動可能なプログラムにおける起動優先順位を判定する。これは、具体的には、ステップＳ

６１２において選択された複数の起動可能なコンテンツデータのヘッダ中の取扱情報に含まれる優先情報を比較して最も高い優先順位を選択する処理である。

【０４８３】

次にステップＳ６１４で選択されたプログラムを起動する。なお、複数の起動可能なプログラムにおいて設定された優先順位が同じである場合には、記録デバイス間でデフォルトの優先順位を設定し、最優先されるデバイスに格納されたコンテンツプログラムを実行する。

【０４８４】

図５８には、複数の記録デバイスに識別子を設定し、各識別子の付された記録デバイスについて順次、認証処理、コンテンツプログラム検索を実行する処理態様、すなわち起動可能コンテンツが複数ある場合の処理例（２）を示した。

【０４８５】

ステップＳ６２１では、記録再生器３００に装着された記録デバイス（ｉ）の認証処理（図２０参照）を実行するステップである。複数(ｎ個)の記録デバイスには順次１～ｎの識別子が付与されている。

【０４８６】

ステップＳ６２２では、ステップＳ６２１での認証が成功したか否かを判定し、認証が成功した場合は、ステップＳ６２３に進み、その記録デバイス（ｉ）の記録媒体中から起動可能プログラムを検索する。認証が成功しなかった場合は、ステップＳ６２７に進み、新たコンテンツ検索可能な記録デバイスの有無を判定し、無い場合は処理を終了し、記録デバイスが存在する場合は、ステップＳ６２８に進み記録デバイス識別子ｉを更新し、ステップＳ６２１以降の認証処理ステップを繰り返す。

【０４８７】

ステップＳ６２３における処理は、記録デバイス（ｉ）に格納されたコンテンツデータから起動可能なプログラムを検出する処理である。これは、具体的には、コンテンツデータの取扱方針に含まれるコンテンツタイプがプログラムであるものを抽出する処理として実行される。

【０４８８】

ステップＳ６２４では、コンテンツタイプがプログラムであるものが抽出されたか否かを判定し、抽出された場合は、ステップＳ６２５において、抽出プログラム中最も優先順位の高いものを選択し、ステップＳ６２６において選択プログラムを実行する。

【０４８９】

ステップＳ６２４において、コンテンツタイプがプログラムであるものが抽出されなかったと判定された場合には、ステップＳ６２７に進み、新たなコンテンツ検索な記録デバイスの有無を判定し、無い場合は処理を終了し、記録デバイスが存在する場合は、ステップＳ６２８に進み記録デバイス識別子ｉを更新し、ステップＳ６２１以降の認証処理ステップを繰り返す。

【０４９０】

図５９は、起動可能コンテンツが複数ある場合の処理例（３）を示す処理フローである。ステップＳ６５１は、記録再生器３００がアクセス可能な記録デバイスの認証処理を実行するステップである。アクセス可能なＤＶＤ装置、ＣＤドライブ、ハードディスク装置、メモリカード、ゲームカートリッジ等の認証処理を実行する。認証処理は、図２で示す制御部３０１の制御のもとに各記録デバイスに対して例えば先に図２０で説明した手順に従って実行される。

【０４９１】

次に、ステップＳ６５２おいて、認証に成功した記録デバイス内のメモリに格納されたコンテンツデータから起動可能なプログラムを検出する。これは、具体的には、コンテンツデータの取扱方針に含まれるコンテンツタイプがプログラムであるものを抽出する処理として実行される。

【０４９２】

次に、ステップＳ６５３において、ステップＳ６５２で抽出された起動可能なプログラムの名称等の情報を表示手段に表示する。なお、表示手段は図２では示されていないが、ＡＶ出力データとして出力されたデータが図示しない表示手段に出力される構成となっている。なお、各コンテンツデータのプログラム名等のユーザ提供情報は、コンテンツデータの識別情報中に格納されており、図２に示すメインＣＰＵ１０６の制御のもとに制御部３０１を介して認証済みの各コンテ

ンツデータのプログラム名称等、プログラム情報を出力手段に出力する。

【０４９３】

次にステップＳ６５４では、図２に示す入力インタフェース、コントローラ、マウス、キーボード等の入力手段からのユーザによるプログラム選択入力を入力インタフェース１１０を介してメインＣＰＵ１０６が受領し、選択入力にしたがって、ステップＳ６５５においてユーザ選択プログラムを実行する。

【０４９４】

このように本発明のデータ処理装置では、コンテンツデータ中のヘッダ内の取扱情報にプログラム起動優先順位情報を格納し、記録再生器３００がこの優先順位に従ってプログラムを起動する、あるいは表示手段に起動プログラム情報を表示してユーザによって選択する構成としたので、ユーザがプログラムを検索する必要がなく、起動に要する時間およびユーザの労力を省くことが可能となる。また、起動可能なプログラムは、すべて記録デバイスの認証処理後に起動、または起動可能プログラムであることの表示がなされるので、プログラムを選択してから正当性の確認を行なう等の処理の煩雑性が解消される。

【０４９５】

（１５）コンテンツ構成および再生（伸長）処理

本発明のデータ処理装置では、上述したように記録再生器３００は、メディア５００または通信手段６００からコンテンツをダウンロード、あるいは記録デバイス４００から再生処理を行う。上記の説明は、コンテンツのダウンロード、あるいは再生処理に伴う、暗号化データの処理を中心として説明してきた。

【０４９６】

図３の記録再生器３００における制御部３０１は、コンテンツデータを提供するＤＶＤ等のデバイス５００、通信手段６００、記録デバイスからのコンテンツデータのダウンロード処理、または再生処理に伴う認証処理、暗号化、復号化処理全般を制御する。

【０４９７】

これらの処理結果として得られた再生可能なコンテンツは、例えば音声データ、画像データ等である。復号データは制御部３０１から図２に示すメインＣＰＵ

の制御下に置かれ、音声データ、画像データ等に応じてＡＶ出力部に出力される。しかし、コンテンツが例えば音声データであってＭＰ３圧縮がなされていれば、図２に示すＡＶ出力部のＭＰ３デコーダによって音声データの復号処理がなされて出力される。また、コンテンツデータが画像データであり、ＭＰＥＧ２圧縮画像であれば、ＡＶ処理部のＭＰＥＧ２デコーダによって伸長処理が実行されて出力されることになる。このように、コンテンツデータに含まれるデータは、圧縮（符号化）処理がなされている場合もあり、また圧縮処理の施されていないデータもあり、コンテンツに応じた処理を施して出力する。

【０４９８】

しかしながら、圧縮処理、伸長処理プログラムには、様々な種類があり、コンテンツプロバイダから圧縮データを提供されても対応する伸長処理実行プログラムが無い場合は、これを再生することができないという事態が発生する。

【０４９９】

そこで、本発明のデータ処理装置は、データコンテンツ中に、圧縮データとその復号（伸長）処理プログラムを併せて格納する構成、あるいは圧縮データと復号（伸長）処理プログラムとのリンク情報をコンテンツデータのヘッダ情報として格納する構成を開示する。

【０５００】

図２に示したデータ処理全体図から、本構成に関する要素および関連要素を簡潔にまとめた図を図６０に示す。記録再生器３００は、例えばＤＶＤ，ＣＤ等のデバイス５００、または通信手段６００、あるいはコンテンツを格納したメモリカード等の記録デバイス４００から様々なコンテンツの提供を受ける。これらのコンテンツは、音声データ、静止画像、動画像データ、プログラムデータ等であり、また暗号化処理の施されているもの、施されていないもの、また、圧縮処理がなされているもの、なされていないもの等、様々なデータが含まれる。

【０５０１】

受領コンテンツが暗号化されている場合は、すでに上述した項目中で説明したような手法によって制御部３０１の制御、および暗号処理部３０２の暗号処理によって復号処理が実行される。復号されたデータはメインＣＰＵ１０６の制御下

で、ＡＶ処理部に１０９に転送されて、ＡＶ処理部１０９のメモリ３０９０に格納された後、コンテンツ解析部３０９１においてコンテンツ構成の解析が実行される。例えばコンテンツ中にデータ伸長プログラムが格納されていれば、プログラム記憶部３０９３にプログラムを格納し、音声データ、画像データ等のデータが含まれていればこれらをデータ記憶部３０９２に記憶する。伸長処理部３０９４では、プログラム記憶部に記憶された例えばＭＰ３等の伸長処理プログラムを用いてデータ記憶部３０９２に記憶された圧縮データの伸長処理を実行して、スピーカ３００１、モニタ３００２に出力される。

【０５０２】

次に、ＡＶ処理部１０９が制御部３０１を介して受領するデータの構成および処理のいくつかの例について説明する。なお、ここでは、コンテンツの例として音声データを示し、また圧縮プログラムの例としてＭＰ３を適用したものを代表して説明するが、本構成は、音声データのみならず、画像データにも適用できるものであり、また、圧縮伸長処理プログラムについてもＭＰ３のみならず、ＭＰＥＧ２，４等各種のプログラムを適用することが可能である。

【０５０３】

図６１にコンテンツ構成例を示す。図６１はＭＰ３によって圧縮された音楽データ６１０２、ＭＰ３復号（伸長）処理プログラム６１０１を併せて１つのコンテンツとして構成した例である。これらのコンテンツは、１コンテンツとしてメディア５００、あるいは記録デバイス４００に格納され、または通信手段６００から配信される。記録再生器３００は、これらのコンテンツが先に説明した通り、暗号化されているものであれば、暗号処理部３０３によって復号処理を実行した後、ＡＶ処理部１０９に転送される。

【０５０４】

ＡＶ処理部１０９のコンテンツ解析部３０９１では、受け取ったコンテンツを解析し、音声データ伸長プログラム（ＭＰ３デコーダ）部と、圧縮音声データ部からなるコンテンツから、音声データ伸長プログラム（ＭＰ３デコーダ）部を取り出してプログラム記憶部３０９３にプログラムを記憶し、圧縮音声データをデータ記憶部３０９２に記憶する。なお、コンテンツ解析部３０９１は、コンテン

ツとは別に受領したコンテンツ名、コンテンツ構成情報等の情報を受領したり、あるいはコンテンツ内に含まれるデータ名等の識別データ、データ長、データ構成等を示すデータに基づいてコンテンツ解析を実行してもよい。次に、圧縮伸長処理部３０９４は、プログラム記憶部３０９３に記憶された音声データ伸長プログラム（ＭＰ３デコーダ）に従ってデータ記憶部３０９２に記憶されたＭＰ３圧縮音声データの伸長処理を実行して、ＡＶ処理部１０９は伸長した音声データをスピーカ３００１に出力する。

【０５０５】

図６２に図６１のコンテンツ構成を持つデータの再生処理の一例を示すフローを示す。ステップＳ６７１は、ＡＶ処理部１０９のメモリ３０９０に格納されたデータ名、例えば音楽データのコンテンツであれば曲名等の情報をコンテンツとは別に受領した情報、あるいはコンテンツ内のデータから取り出し、モニタ３００２に表示する。ステップＳ６７２は、ユーザの選択をスイッチ、キーボード等の各種入力手段から入力インタフェース１１０を介して受領し、ＣＰＵ１０６の制御のもとにユーザ入力データに基づく再生処理命令をＡＶ処理部１０９に出力する。ＡＶ処理部１０９は、ステップＳ６７３においてユーザ選択によるデータの抽出、伸長処理を実行する。

【０５０６】

次に図６３に、１つのコンテンツには圧縮音声データ、あるいは伸長処理プログラムのいずれか一方が含まれ、さらに各コンテンツのヘッダ情報としてコンテンツの内容を示すコンテンツ情報が含まれる構成例を示す。

【０５０７】

図６３に示すように、コンテンツがプログラム６２０２である場合は、ヘッダ情報６２０１としてプログラムであること、およびプログラム種類がＭＰ３伸長プログラムであることを示すコンテンツ識別情報が含まれる。一方、音声データ６２０４をコンテンツとして含む場合は、ヘッダ６２０３のコンテンツ情報にはＭＰ３圧縮データであるとの情報が含まれる。このヘッダ情報は、前述した例えば図４に示すコンテンツデータ構成の取扱方針（図５参照）中に含まれるデータから再生に必要な情報のみを選択してＡＶ処理部１０９へ転送するコンテンツに

付加して構成することが可能である。具体的には、図５に示す「取扱方針」中の各構成データに暗号処理部３０２において必要となる取扱方針データと、ＡＶ処理部１０９における再生処理時に必要となるデータとの識別値を付加し、これら識別値が、ＡＶ処理部１０９において必要であることを示すもののみを抽出してヘッダ情報とすることができる。

【０５０８】

図６３に示す各コンテンツを受領したＡＶ処理部１０９のコンテンツ解析部３０９１は、ヘッダ情報に従って、プログラムである場合はプログラムコンテンツをプログラム記憶部３０９３に記憶し、データである場合は、データコンテンツをデータ記憶部３０９２に記憶する。その後、圧縮伸長処理部３０９４は、データ記憶部からデータを取り出して、プログラム記憶部３０９３に記憶したＭＰ３プログラムに従って伸長処理を実行して出力する。なお、プログラム記憶部３０９３にすでに同一プログラムが格納されている場合は、プログラム格納処理は省略してもよい。

【０５０９】

図６４に図６３のコンテンツ構成を持つデータの再生処理の一例を示すフローを示す。ステップＳ６７５は、ＡＶ処理部１０９のメモリ３０９０に格納されたデータ名、例えば音楽データのコンテンツであれば曲名等の情報をコンテンツとは別に受領した情報、あるいはコンテンツ内のヘッダから取り出し、モニタ３００２に表示する。ステップＳ６７６は、ユーザの選択をスイッチ、キーボード等の各種入力手段から入力インタフェース１１０を介して受領する。

【０５１０】

次に、ステップＳ６７７では、ユーザ選択に対応するデータの再生用プログラム（例えばＭＰ３）を検索する。このプログラム検索対象は、記録再生機器３００のアクセス可能な範囲を最大検索範囲とすることが好ましく、例えば図６０に示す、各メディア５００、通信手段６００、記録デバイス４００等も検索範囲とする。

【０５１１】

ＡＶ処理部１０９に渡されるコンテンツはデータ部のみであり、プログラムコ

ンテンツは記録再生器３００内の他の記録媒体に格納される場合もあり、ＤＶＤ、ＣＤ等のメディアを介してコンテンツ提供業者から提供されることもある。従って、検索対象を記録再生機器３００のアクセス格納な範囲を検索範囲とする。検索の結果として再生プログラムが見つかると、ＣＰＵ１０６の制御のもとにユーザ入力データに基づく再生処理命令をＡＶ処理部１０９に出力する。ＡＶ処理部１０９は、ステップＳ６７９においてユーザ選択によるデータの抽出、伸長処理を実行する。また、別の実施例として、プログラムの検索をステップＳ６７５より前に行い、ステップＳ６７５においては、プログラムが検出されたデータのみを表示するようにしてもよい。

【０５１２】

次に図６５に、１つのコンテンツに圧縮音声データ６３０３、伸長処理プログラム６３０２が含まれ、さらにコンテンツのヘッダ情報６３０１としてコンテンツの再生優先順位情報が含まれる構成例を示す。これは、先の図６１のコンテンツ構成にヘッダ情報として再生優先順位情報を付加した例である。これは、前述の「（１４）コンテンツデータにおける取扱方針中の起動優先順位に基づくプログラム起動処理」と同様、ＡＶ処理部１０９が受領したコンテンツ間において設定された再生優先順位に基づいて再生順を決定するものである。

【０５１３】

図６６に図６５のコンテンツ構成を持つデータの再生処理の一例を示すフローを示す。ステップＳ６８１は、ＡＶ処理部１０９のメモリ３０９０に格納されたデータ、すなわち再生対象データのデータ情報を検索リストに設定する。検索リストはＡＶ処理部１０９内のメモリの一部領域を使用して設定する。次に、ステップＳ６８２において、ＡＶ処理部１０９のコンテンツ解析部３０９１において検索リストから優先順位の高いデータを選択し、ステップＳ６８３において、選択されたデータの再生処理を実行する。

【０５１４】

次に図６７に、１つのコンテンツにヘッダ情報とプログラムデータ６４０２、あるいはヘッダ情報６４０３と、圧縮データ６４０４のいずれかの組合せから成る例において、データコンテンツのヘッダ６４０３にのみ、再生優先順位情報が

付加されている構成例を示す。

【０５１５】

図６８に図６７のコンテンツ構成を持つデータの再生処理の一例を示すフローを示す。ステップＳ６９１は、ＡＶ処理部１０９のメモリ３０９０に格納されたデータ、すなわち再生対象データのデータ情報を検索リストに設定する。検索リストはＡＶ処理部１０９内のメモリの一部領域を使用して設定する。次に、ステップＳ６９２において、ＡＶ処理部１０９のコンテンツ解析部３０９１において検索リストから優先順位の高いデータを選択する。

【０５１６】

次に、ステップＳ６９３では、選択されたデータに対応するデータ再生用プログラム（例えばＭＰ３）を検索する。このプログラム検索対象は、先の図６４のフローにおける処理と同様、記録再生機器３００のアクセス格納な範囲を最大検索範囲とすることが好ましく、例えば図６０に示す各メディア５００、通信手段６００、記録デバイス４００等も検索範囲とする。

【０５１７】

検索の結果として再生プログラムが見つかる（ステップＳ６９４でＹｅｓ）と、ステップＳ６９５において、選択されたデータを検索の結果得られたプログラムを用いて、伸長再生処理を実行する。

【０５１８】

一方、検索結果としてプログラムが検出されなかった場合（ステップＳ６９４でＹｅｓ）は、ステップＳ６９６に進み、ステップＳ６９１で設定した検索リスト中に含まれる他のデータにおいて、同一のプログラムを用いた再生処理が必要なものを削除する。これは、新たにそのデータに対する再生プログラム検索を実行しても検出されないことが明らかであるからである。さらに、ステップＳ６９７において検索リストが空であるかを判定し、からでない場合は、ステップＳ６９２に戻り、さらに次の優先順位の高いデータを抽出して、プログラム検索処理を実行する。

【０５１９】

このように、本構成によれば、圧縮処理されたコンテンツは、その復号(伸長)

ブログラムと共に構成されるか、あるいはコンテンツが圧縮されたデータのみ、あるいは伸長処理プログラムのみである場合は、それぞれのコンテンツにコンテンツがどのような圧縮データであるのか、あるいはどのような処理を実行するかを示すヘッダ情報を有しているので、コンテンツを受領した処理部（例えばＡＶ処理部）は、圧縮データに付属する伸長処理プログラムを用いて伸長再生処理を実行するか、あるいは伸長処理プログラムを圧縮データのヘッダ情報に基づいて検索して、検索の結果得られたプログラムにしたがって伸長再生処理を実行するので、ユーザによるデータの伸長プログラムの選択、検索等の処理が不要となりユーザ負担が軽減され、効率的なデータ再生が可能となる。さらに、ヘッダに再生優先順位情報を有した構成によれば、再生順序を自動設定する構成が可能となり、ユーザによる再生順設定の操作を省略することができる。

【０５２０】

なお、上述の実施例では、圧縮音声データコンテンツ、および音声圧縮データの伸長処理プログラムとしてのＭＰ３を例として説明したが、圧縮データを含むコンテンツ、圧縮画像データの伸長処理プログラムを有するコンテンツであっても本構成は同様に適用可能であり、同様の効果を奏するものである。

【０５２１】

（１６）セーブデータの生成および記録デバイスへの格納、再生処理

本発明のデータ処理装置は、例えば記録再生器３００において実行されるコンテンツがゲームプログラム等である場合等、ゲームプログラムを途中で中断して、所定時間後、新たに再開したい場合には、その中断時点のゲーム状態等をセーブ、すなわち記録デバイスに格納し、これを再開時に読み出してゲームを続行することが可能な構成を持つ。

【０５２２】

従来のゲーム機器、パソコン等の記録再生器におけるセーブデータ保存構成は、例えば記録再生器に内蔵、あるいは外付け可能なメモリカード、フロッピーディスク、ゲームカートリッジ、あるいはハードディスク等の記憶媒体にセーブデータを保存する構成を持つが、特に、そのセーブデータに対するセキュリティ確保構成を有しておらず、例えばゲームアプリケーションプログラムに共通の仕様

でデータのセーブ処理が行われる構成となっている。

【０５２３】

従って、例えばある１つの記録再生器Ａを用いてセーブされたセーブデータが別のゲームプログラムによって使用されたり、書換えられたりする事態が発生し、従来、セーブデータのセキュリティはほとんど考慮されていなかったのが実状である。

【０５２４】

本発明のデータ処理装置は、このようなセーブデータのセキュリティ確保を実現可能とした構成を提供する。例えばあるゲームプログラムのセーブデータは、そのゲームプログラムのみが使用可能な情報に基づいて暗号化して記録デバイスに格納する。あるいは、記録再生器固有の情報に基づいて暗号化して記録デバイスに格納する。これらの手法により、セーブデータの利用を特定の機器、特定のプログラムのみに制限することができ、セーブデータのセキュリティが確保される。以下、本発明のデータ処理装置における「セーブデータの生成および記録デバイスへの格納、再生処理」について説明する。

【０５２５】

図６９に本発明のデータ処理装置におけるセーブデータ格納処理について説明するブロック図を示す。ＤＶＤ，ＣＤ等のメディア５００、あるいは通信手段６００からコンテンツが記録再生器３００に提供される。提供されるコンテンツは、先に説明したようにコンテンツ固有の鍵であるコンテンツ鍵Ｋｃｏｎによって暗号化されており、記録再生器３００は、前述した「（７）記録再生器から記録デバイスへのダウンロード処理」の欄で説明（図２２参照）した処理に従ってコンテンツ鍵を取得して、暗号化コンテンツを復号した後、記録デバイス４００に格納する。ここでは、記録再生器３００がコンテンツプログラムをメディア、通信手段から復号して再生、実行を行ない、実行の後、得られるセーブデータを外付け、あるいは内蔵のメモリカード、ハードディスク等の各種の記録デバイス４００Ａ、４００Ｂ、４００Ｃのいずれかに格納し、再生する処理、あるいはコンテンツを記録デバイス４００Ａにダウンロードした後、記録デバイス４００Ａからコンテンツを再生、実行して、そのセーブデータを外付け、あるいは内蔵のメ

モリカード、ハードディスク等の各種の記録デバイス４００Ａ、４００Ｂ、４００Ｃのいずれかに格納する処理記録デバイス４００に格納し、再生する処理について説明する。

【０５２６】

記録再生器３００には、先に説明したように記録再生器識別子ＩＤｄｅｖ、システムに共通な署名鍵であるシステム署名鍵Ｋｓｙｓ、個々の記録再生器に固有の署名鍵である記録再生器署名鍵Ｋｄｅｖ、さらに各種の個別鍵を生成するマスタ鍵を有する。マスタ鍵については、「（１２）マスタ鍵に基づく暗号処理鍵生成構成」において、詳しく説明した通り、例えば、配送鍵Ｋｄｉｓ、あるいは認証鍵Ｋａｋｅ等を生成する鍵である。ここでは、特にマスタ鍵の種類を限定することなく記録再生器３００の有するマスタ鍵全般を代表するものとしてＭＫｘとして示す。図６９の下段には、セーブデータの暗号鍵Ｋｓａｖの例を示した。セーブデータ暗号鍵Ｋｓａｖは、セーブデータを各種記録デバイス４００Ａ～Ｃに格納する場合の暗号化処理、そして、各種記録デバイス４００Ａ～Ｃから再生する際の復号処理に用いられる暗号鍵である。図７０以下を用いて、セーブデータの格納処理および再生処理の例を説明する。

【０５２７】

図７０は、コンテンツ個有鍵、システム共通鍵のいずれかを用いてセーブデータを記録デバイス４００Ａ～Ｃいずれかに格納する処理のフロー図である。なお、各フローにおける処理は記録再生器３００が実行する処理であり、各フローでセーブデータを格納する記録デバイスは内蔵、外付け記録デバイス４００Ａ～Ｃのいずれかであればよく、いずれかに限定さるものではない。

【０５２８】

ステップＳ７０１は、コンテンツ識別子、例えばゲームＩＤを記録再生器３００が読み出す処理である。これは、先に説明した図４、２６、２７、３２～３５に示すコンテンツデータ中の識別情報に含まれるデータであり、セーブデータの格納処理命令を図２に示す入力インタフェース１１０を介して受領したメインＣＰＵ１０６がコンテンツ識別子の読み取りを制御部３０１に指示する。

【０５２９】

制御部３０１は、実行プログラムがＤＶＤ、ＣＤ－ＲＯＭ等、読取部３０４を介して実行されているコンテンツの場合は、読取部３０４を介してコンテンツデータ中のヘッダに含まれる識別情報を取り出し、実行プログラムが、記録デバイス４００に格納されたコンテンツである場合は、記録デバイスコントローラ３０３を介して識別情報を取り出す。なお、記録再生器３００がコンテンツプログラムを実行中で、すでに記録再生器中のＲＡＭ、その他のアクセス可能な記録媒体にコンテンツ識別子が格納済みである場合は、新たな読み取り処理を実行せずに、読み込み済みデータに含まれる識別情報を利用してもよい。

【０５３０】

次に、ステップＳ７０２は、プログラムの使用制限を行なうか否かによって処理を変更するステップである。プログラム使用制限とは、保存するセーブデータをそのプログラムのみに固有に利用可能とする制限を付するか否かを設定する制限情報であり、プログラムのみに固有に利用可能とする場合は、「プログラム使用制限あり」とし、プログラムに利用を拘束されないセーブデータとする場合を「プログラム使用制限なし」とする。これは、ユーザが任意に設定できるようにしてもよいし、コンテンツ製作者が設定して、この情報をコンテンツプログラム中に格納しておいてもよく、設定された制限情報は、図６９の記録デバイス４００Ａ～Ｃにデータ管理ファイルとして格納される。

【０５３１】

データ管理ファイルの例を図７１に示す。データ管理ファイルは項目としてデータ番号、コンテンツ識別子、記録再生器識別子、プログラム使用制限を含むテーブルとして生成される。コンテンツ識別子は、セーブデータを格納する対象となったコンテンツプログラムの識別データである。記録再生器識別子は、セーブデータを格納した記録再生器の識別子、例えば図６９に示す［ＩＤｄｅｖ］である。プログラム使用制限は、上述したように保存するセーブデータをそのプログラムのみに固有に利用可能とす場合、「する」の設定とし、対応プログラムに制限されない利用を可能とする場合「しない」の設定となる。プログラム使用制限は、コンテンツプログラムを利用するユーザが任意に設定できるようにしてもよいし、コンテンツ製作者が設定して、この情報をコンテンツプログラム中に格納

しておいてもよい。

【０５３２】

図７０に戻り、フローの説明を続ける。ステップＳ７０２において、プログラム使用制限について「する」の設定がされている場合は、ステップＳ７０３に進む。ステップＳ７０３では、コンテンツデータからコンテンツ固有の鍵、例えば先に説明したコンテンツ鍵Ｋｃｏｎを読み出してコンテンツ固有鍵をセーブデータ暗号鍵Ｋｓａｖとするか、あるいはコンテンツ固有鍵に基づいてセーブデータ暗号鍵Ｋｓａｖを生成する。

【０５３３】

一方、ステップＳ７０２において、プログラム使用制限について「しない」の設定がされている場合は、ステップＳ７０７に進む。ステップＳ７０７では、記録再生器３００内に格納されたシステム共通鍵、例えばシステム署名鍵Ｋｓｙｓを記録再生器３００の内部メモリ３０７から読み出して、システム署名鍵Ｋｓｙｓをセーブデータ暗号鍵Ｋｓａｖとするか、あるいはシステム署名鍵に基づいてセーブデータ暗号鍵Ｋｓａｖを生成する。または、別途、記録再生器３００の内部メモリ３０７内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ｋｓａｖとして使用してもよい。

【０５３４】

次に、ステップＳ７０４において、ステップＳ７０３、またはステップＳ７０７で選択、または生成されたセーブデータ暗号化鍵Ｋｓａｖを用いてセーブデータの暗号化処理を実行する。この暗号化処理は、図２における暗号処理部３０２が例えば前述のＤＥＳアルゴリズムを適用して実行する。

【０５３５】

ステップＳ７０４において暗号化処理されたセーブデータは、ステップＳ７０５において記録デバイスに格納される。セーブデータを格納可能な記録デバイスが図６９に示すように複数ある場合は、ユーザが記録デバイス４００Ａ～Ｃのいずれかをセーブデータ格納先として予め選択する。さらに、ステップＳ７０６において先に図７１を用いて説明したデータ管理ファイルに先にステップＳ７０２で設定したプログラム使用制限情報の書き込み、すなわちプログラム使用制限「

する」または「しない」の書き込みを実行する。

【０５３６】

以上で、セーブデータの格納処理が終了する。ステップＳ７０２においてＹｅｓ、すなわち「プログラム使用制限する」の選択がなされ、ステップＳ７０３においてコンテンツ固有鍵に基づいて生成されたセーブデータ暗号化鍵Ｋｓａｖによって暗号化処理されたセーブデータは、コンテンツ固有鍵情報を持たないコンテンツプログラムによる復号処理が不可能となり、セーブデータは同じコンテンツ鍵情報を有するコンテンツプログラムのみが利用できることになる。ただし、ここでは、セーブデータ暗号化鍵Ｋｓａｖは記録再生器固有の情報に基いて生成されたものではないので、例えばメモリカード等の着脱可能な記録デバイスに格納されたセーブデータは異なる記録再生器においても対応するコンテンツプログラムと共に使用する限り再生可能となる。

【０５３７】

また、ステップＳ７０２においてＮｏ、すなわち「プログラム使用制限しない」の選択がなされ、ステップＳ７０７においてシステム共通鍵に基づくセーブデータ暗号化鍵Ｋｓａｖによって暗号化処理されたセーブデータは、コンテンツ識別子が異なるプログラムを用いた場合でも、また、記録再生器が異なっていた場合でも再生して利用することが可能となる。

【０５３８】

図７２は、図７０のセーブデータ格納処理によって格納されたセーブデータを再生する処理を示したフローである。

【０５３９】

ステップＳ７１１は、コンテンツ識別子、例えばゲームＩＤを記録再生器３００が読み出す処理である。これは、先に説明した図７０のセーブデータ格納処理のステップＳ７０１と同様の処理であり、コンテンツデータ中の識別情報に含まれるデータを読み出す処理である。

【０５４０】

次に、ステップＳ７１２では、図６９に示す記録デバイス４００Ａ～Ｃから、図７１を用いて説明したデータ管理ファイルを読み出し、ステップＳ７１１にお

いて読み出したコンテンツ識別子、および対応して設定された使用プログラム制限情報を抽出する。データ管理ファイルに設定されたプログラム使用制限が「する」であった場合は、ステップＳ７１４に進み、「しない」であった場合には、ステップＳ７１７に進む。

【０５４１】

ステップＳ７１４では、コンテンツデータからコンテンツ固有の鍵、例えば先に説明したコンテンツ鍵Ｋｃｏｎを読み出してコンテンツ固有鍵をセーブデータ復号化鍵Ｋｓａｖとするか、あるいはコンテンツ固有鍵に基づいてセーブデータ復号化鍵Ｋｓａｖを生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、あるコンテンツ固有鍵に基づいて暗号化されたデータは、同一のコンテンツ固有鍵に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。

【０５４２】

一方、ステップＳ７１２において、データ管理ファイルの設定がプログラム使用制限について「しない」の設定であった場合は、ステップＳ７１７において、記録再生器３００内に格納されたシステム共通鍵、例えばシステム署名鍵Ｋｓｙｓを記録再生器３００の内部メモリ３０７から読み出して、システム署名鍵Ｋｓｙｓをセーブデータ復号化鍵Ｋｓａｖとするか、あるいはシステム署名鍵に基づいてセーブデータ復号化鍵Ｋｓａｖを生成する。または、別途、記録再生器３００の内部メモリ３０７内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ｋｓａｖとして使用してもよい。

【０５４３】

次に、ステップＳ７１５において、ステップＳ７１４、またはステップＳ７１７で選択、または生成されたセーブデータ復号化鍵Ｋｓａｖを用いてセーブデータの復号化処理を実行し、ステップＳ７１６において、復号したセーブデータを記録再生器３００において再生、実行する。

【０５４４】

以上で、セーブデータの再生処理が終了する。上述のようにデータ管理ファイルに「プログラム使用制限する」の設定がなされている場合は、コンテンツ固有

鍵に基づいてセーブデータ復号化鍵が生成され、「プログラム使用制限しない」の設定がある場合はシステム共通鍵に基づいてセーブデータ復号化鍵が生成される。「プログラム使用制限する」の設定がされている場合、使用しているコンテンツのコンテンツ識別子が同じものでないとセーブデータの復号処理の可能な復号化鍵を得ることができないこととなり、セーブデータのセキュリティを高めることが可能となる。

【０５４５】

図７３、図７４は、コンテンツ識別子を用いてセーブデータの暗号化鍵、復号化鍵を生成するセーブデータ格納処理フロー（図７３）、セーブデータ再生処理フロー（図７４）である。

【０５４６】

図７３において、ステップＳ７２１～Ｓ７２２は、図７０のステップＳ７０１～Ｓ７０２と同様の処理であり、説明を省略する。

【０５４７】

図７３のセーブデータ格納処理フローは、ステップＳ７２２において「プログラム使用制限する」の設定を行なった場合、ステップＳ７２３においてコンテンツデータからコンテンツ識別子、すなわちコンテンツＩＤを読み出してコンテンツＩＤをセーブデータ暗号化鍵Ｋｓａｖとするか、あるいはコンテンツＩＤに基づいてセーブデータ暗号化鍵Ｋｓａｖを生成する。例えば、記録再生器３００の暗号処理部３０７はコンテンツデータから読み出したコンテンツＩＤに、記録再生器３００の内部メモリに格納されたマスター鍵ＭＫｘを適用して、例えばＤＥＳ（ＭＫｘ，コンテンツＩＤ）によってセーブデータ暗号化鍵Ｋｓａｖを得ることができる。または、別途、記録再生器３００の内部メモリ３０７内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ｋｓａｖとして使用してもよい。

【０５４８】

一方、ステップＳ７２２において、プログラム使用制限について「しない」の設定とした場合は、ステップＳ７２７において、記録再生器３００内に格納されたシステム共通鍵、例えばシステム署名鍵Ｋｓｙｓを記録再生器３００の内部メ

モリ３０７から読み出して、システム署名鍵Ｋｓｙｓをセーブデータ暗号化鍵Ｋｓａｖとするか、あるいはシステム署名鍵に基づいてセーブデータ暗号化鍵Ｋｓａｖを生成する。または、別途、記録再生器３００の内部メモリ３０７内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ｋｓａｖとして使用してもよい。

【０５４９】

ステップＳ７２４以下の処理は、前述の図７０の処理フローにおけるステップＳ７０４以下の処理と同様であり、説明を省略する。

【０５５０】

さらに、図７４は、図７３のセーブデータ格納処理フローで記録デバイスに格納されたセーブデータを再生、実行する処理フローであり、ステップＳ７３１～Ｓ７３３は前述の図７２の対応処理と同様であり、ステップＳ７３４のみが異なる。ステップＳ７３４においては、コンテンツデータからコンテンツ識別子、すなわちコンテンツＩＤを読み出してコンテンツＩＤをセーブデータ復号化鍵Ｋｓａｖとするか、あるいはコンテンツＩＤに基づいてセーブデータ復号化鍵Ｋｓａｖを生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、あるコンテンツ識別子に基づいて暗号化されたデータは、同一のコンテンツ識別子に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。

【０５５１】

以下の処理、ステップＳ７３５、Ｓ７３６、Ｓ７３７は、図７２の対応処理と同様であるので説明を省略する。図７３、図７４のセーブデータ格納および再生処理に従えば、プログラム使用制限するの設定を行なった場合、コンテンツＩＤを使用してセーブデータ暗号化鍵、復号化鍵を生成する構成としたので、先のコンテンツ固有鍵を使用したセーブデータ格納、再生処理と同様、対応するコンテンツプログラムが整合する場合以外は、セーブデータを利用することができない構成となり、セーブデータセキュリティを高めた保存が可能となる。

【０５５２】

図７５、図７７は、記録再生器固有鍵を用いてセーブデータの暗号化鍵、復号

化鍵を生成するセーブデータ格納処理フロー（図７５）、セーブデータ再生処理フロー（図７７）である。

【０５５３】

図７５において、ステップＳ７４１は、図７０のステップＳ７０１と同様の処理であり、説明を省略する。ステップＳ７４２は、記録再生器の制限をするかしないかを設定するステップである。記録再生器制限は、セーブデータを利用可能な記録再生器を限定する場合、すなわちセーブデータを生成し格納した記録再生器にのみ利用可能とする場合を「する」と設定し、他の記録再生器でも利用可能とする場合を「しない」の設定とするものである。ステップＳ７４２において「記録再生器制限する」の設定をすると、ステップＳ７４３に進み、「しない」の設定をするとステップＳ７４７に進む。

【０５５４】

データ管理ファイルの例を図７６に示す。データ管理ファイルは項目としてデータ番号、コンテンツ識別子、記録再生器識別子、記録再生器制限を含むテーブルとして生成される。コンテンツ識別子は、セーブデータを格納する対象となったコンテンツプログラムの識別データである。記録再生器識別子は、セーブデータを格納した記録再生器の識別子、例えば図６９に示す［ＩＤｄｅｖ］である。記録再生器制限は、セーブデータを利用可能な記録再生器を限定する場合、すなわちセーブデータを生成し格納した記録再生器にのみ利用可能とする場合を「する」と設定し、他の記録再生器でも利用可能とする場合を「しない」の設定とするものである。記録再生器制限情報は、コンテンツプログラムを利用するユーザが任意に設定できるようにしてもよいし、コンテンツ製作者が設定して、この情報をコンテンツプログラム中に格納しておいてもよい。

【０５５５】

図７５のセーブデータ格納処理フローにおいては、ステップＳ７４２において「記録再生器制限する」の設定を行なった場合、ステップＳ７４３において記録再生器３００から記録再生器固有鍵、例えば記録再生器署名鍵Ｋｄｅｖを記録再生器３００の内部メモリ３０７から読み出して記録再生器署名鍵Ｋｄｅｖをセーブデータ暗号化鍵Ｋｓａｖとするか、あるいは記録再生器署名鍵Ｋｄｅｖに基づ

いてセーブデータ暗号化鍵Ｋｓａｖを生成する。または、別途、記録再生器３００の内部メモリ３０７内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ｋｓａｖとして使用してもよい。

【０５５６】

一方、ステップＳ７４２において、記録再生器制限について「しない」の設定とした場合は、ステップＳ７４７において、記録再生器３００内に格納されたシステム共通鍵、例えばシステム署名鍵Ｋｓｙｓを記録再生器３００の内部メモリ３０７から読み出して、システム署名鍵Ｋｓｙｓをセーブデータ暗号化鍵Ｋｓａｖとするか、あるいはシステム署名鍵に基づいてセーブデータ暗号化鍵Ｋｓａｖを生成する。または、別途、記録再生器３００の内部メモリ３０７内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ｋｓａｖとして使用してもよい。

【０５５７】

ステップＳ７４４、Ｓ７４５の処理は、前述の図７０の処理フローにおける対応処理と同様であり、説明を省略する。

【０５５８】

ステップＳ７４６では、データ管理ファイル（図７６参照）にコンテンツ識別子、記録再生器識別子、そしてステップ７４２でユーザが設定した記録再生器制限情報「する／しない」を書き込む。

【０５５９】

さらに、図７７は、図７５のセーブデータ格納処理フローで記録デバイスに格納されたセーブデータを再生、実行する処理フローであり、ステップＳ７５１は前述の図７２の対応処理と同様、コンテンツ識別子を読み出す。次に、ステップＳ７５２においては、記録再生器３００内のメモリに格納された記録再生器識別子（ＩＤｄｅｖ）を読み出す。

【０５６０】

ステップＳ７５３では、データ管理ファイル（図７６参照）からコンテンツ識別子、記録再生器識別子、設定済みの記録再生器制限情報「する／しない」の各情報を読み出す。データ管理ファイル中のコンテンツ識別子が一致するエントリ

において、記録再生器制限情報が「する」に設定されている場合、テーブルエントリの記録再生器識別子がステップＳ７５２で読み取られた記録再生器識別子と異なる場合は処理を終了する。

【０５６１】

次に、ステップＳ７５４でデータ管理ファイルの設定が「記録再生器制限する」である場合は、ステップＳ７５５に進み、「しない」である場合は、ステップＳ７５８に進む。

【０５６２】

ステップＳ７５５においては、記録再生器３００から記録再生器固有鍵、例えば記録再生器署名鍵Ｋｄｅｖを記録再生器３００の内部メモリ３０７から読み出して記録再生器署名鍵Ｋｄｅｖをセーブデータ復号化鍵Ｋｓａｖとするか、あるいは記録再生器署名鍵Ｋｄｅｖに基づいてセーブデータ復号化鍵Ｋｓａｖを生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、ある記録再生器固有鍵に基づいて暗号化されたデータは、同一の記録再生器固有鍵に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。または、別途、記録再生器３００の内部メモリ３０７内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ｋｓａｖとして使用してもよい。

【０５６３】

一方ステップＳ７５８においては、記録再生器３００内に格納されたシステム共通鍵、例えばシステム署名鍵Ｋｓｙｓを記録再生器３００の内部メモリ３０７から読み出して、システム署名鍵Ｋｓｙｓをセーブデータ復号化鍵Ｋｓａｖとするか、あるいはシステム署名鍵に基づいてセーブデータ復号化鍵Ｋｓａｖを生成する。または、別途、記録再生器３００の内部メモリ３０７内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ｋｓａｖとして使用してもよい。以下のステップＳ７５６，Ｓ７５７は、前述のセーブデータ再生処理フローの対応ステップと同様の処理である。

【０５６４】

図７５、図７７に示すセーブデータ格納、再生処理フローによれば、「記録再

生器制限する」の選択がなされたセーブデータは、記録再生器固有鍵によって暗号化、復号化処理が実行されるため、同一の記録再生器個有鍵を持つ記録再生器、すなわち同一の記録再生器によってのみ復号して利用することが可能となる。

【０５６５】

次に、図７８、図７９に記録再生器識別子を用いてセーブデータの暗号化、復号化鍵を生成して格納、再生する処理フローを示す。

【０５６６】

図７８は、記録再生器識別子を用いてセーブデータの暗号化を行い記録デバイスに格納する。ステップＳ７６１～Ｓ７６３は、先の図７５と同様の処理である。ステップＳ７６４では、記録再生器から読み出した記録再生器識別子（ＩＤｄｅｖ）を用いてセーブデータの暗号化鍵Ｋｓａｖを生成する。ＩＤｄｅｖをセーブデータ暗号化鍵Ｋｓａｖとして適用するか、あるいは記録再生器３００の内部メモリに格納されたマスター鍵ＭＫｘを適用して、ＤＥＳ（ＭＫｘ，ＩＤｄｅｖ）によってセーブデータ暗号化鍵Ｋｓａｖを得る等、ＩＤｄｅｖに基づいてセーブデータ暗号化鍵ｋｓａｖを生成する。または、別途、記録再生器３００の内部メモリ３０７内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ｋｓａｖとして使用してもよい。

【０５６７】

以下の処理ステップＳ７６５～Ｓ７６８は、前述の図７５の対応処理と同様であり、説明を省略する。

【０５６８】

図７９は、図７８の処理によって記録デバイスに格納されたセーブデータを再生、実行する処理フローである。ステップＳ７７１～Ｓ７７４は、前述の図７７の対応処理と同様である。

【０５６９】

ステップＳ７７５では、記録再生器から読み出した記録再生器識別子（ＩＤｄｅｖ）を用いてセーブデータの復号化鍵Ｋｓａｖを生成する。ＩＤｄｅｖをセーブデータ復号化鍵Ｋｓａｖとして適用するか、あるいは記録再生器３００の内部メモリに格納されたマスター鍵ＭＫｘを適用して、ＤＥＳ（ＭＫｘ，ＩＤｄｅｖ

）によってセーブデータ復号化鍵Ｋｓａｖを得る等、ＩＤｄｅｖに基づいてセーブデータ復号化鍵Ｋｓａｖを生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、ある記録再生器識別子に基づいて暗号化されたデータは、同一の記録再生器識別子に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。または、別途、記録再生器３００の内部メモリ３０７内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ｋｓａｖとして使用してもよい。

【０５７０】

以下の処理ステップＳ７７６～Ｓ７７８は前述の図７６の対応ステップの処理と同様である。

【０５７１】

この図７８、図７９に示すセーブデータ格納、再生処理フローによれば、「記録再生器制限する」の選択がなされたセーブデータは、記録再生器識別子によって暗号化、復号化処理が実行されるため、同一の記録再生器識別子を持つ記録再生器、すなわち同一の記録再生器によってのみ復号して利用することが可能となる。

【０５７２】

次に図８０～８２を用いて、上述のプログラム使用制限、および記録再生器使用制限を併せて実行するセーブデータ格納、再生処理について説明する。

【０５７３】

図８０は、セーブデータ格納処理フローである。ステップＳ７８１において、コンテンツ識別子をコンテンツデータから読み出し、ステップＳ７８２において、プログラム使用制限判定を行ない、ステップＳ７８３において記録再生器制限判定を行なう。

【０５７４】

「プログラム使用制限あり」、かつ「記録再生器制限あり」の場合は、ステップＳ７８５において、コンテンツ固有鍵（ｅｘ．Ｋｃｏｎ）と、記録再生器固有鍵（Ｋｄｅｖ）の双方に基づいてセーブデータ暗号化鍵Ｋｓａｖが生成される。これは、例えばＫｓａｖ＝（Ｋｃｏｎ　ＸＯＲ　Ｋｄｅｖ）、あるいは記録再生

器３００の内部メモリに格納されたマスタ鍵ＭＫｘを適用してＫｓａｖ＝ＤＥＳ（ＭＫｘ，Ｋｃｏｎ　ＸＯＲ　Ｋｄｅｖ）等によって得ることができる。または、別途、記録再生器３００の内部メモリ３０７内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ｋｓａｖとして使用してもよい。

【０５７５】

「プログラム使用制限あり」、かつ「記録再生器制限なし」の場合は、ステップＳ７８６において、コンテンツ固有鍵（ｅｘ．Ｋｃｏｎ）をセーブデータ暗号化鍵Ｋｓａｖとするか、あるいはコンテンツ固有鍵（ｅｘ．Ｋｃｏｎ）に基づいてセーブデータ暗号化鍵Ｋｓａｖを生成する。

【０５７６】

「プログラム使用制限なし」、かつ「記録再生器制限あり」の場合は、ステップＳ７８７において、記録再生器固有鍵（Ｋｄｅｖ）をセーブデータ暗号化鍵Ｋｓａｖとするか、あるいは記録再生器固有鍵（Ｋｄｅｖ）に基づいてセーブデータ暗号化鍵Ｋｓａｖが生成される。または、別途、記録再生器３００の内部メモリ３０７内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ｋｓａｖとして使用してもよい。

【０５７７】

さらに、「プログラム使用制限なし」、かつ「記録再生器制限なし」の場合は、ステップＳ７８７において、システム共通鍵、例えばシステム署名鍵Ｋｓｙｓをセーブデータ暗号化鍵Ｋｓａｖとするか、あるいはシステム署名鍵Ｋｓｙｓに基づいてセーブデータ暗号化鍵Ｋｓａｖを生成する。または、別途、記録再生器３００の内部メモリ３０７内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ｋｓａｖとして使用してもよい。

【０５７８】

ステップＳ７８９では、ステップＳ７８５～Ｓ７８８のいずれかで生成されたセーブデータ暗号化鍵Ｋｓａｖによってセーブデータが暗号化され、記録デバイスに格納される。

【０５７９】

さらに、ステップＳ７９０では、ステップＳ７８２、Ｓ７８３において設定し

た制限情報がデータ管理ファイルに格納される。データ管理ファイルは、例えば図８１に示す構成となり、項目としてデータ番号、コンテンツ識別子、記録再生器識別子、プログラム使用制限、記録再生器制限を含む。

【０５８０】

図８２は、図８０の処理によって記録デバイスに格納されたセーブデータを再生、実行する処理フローである。ステップＳ７９１では、実行プログラムのコンテンツ識別子、記録再生器識別子を読み出し、ステップＳ７９２において、図８１に示すデータ管理ファイルからコンテンツ識別子、記録再生器識別子、プログラム使用制限、記録再生器制限情報を読み出す。この場合、プログラム使用制限が「する」でコンテンツ識別子が不一致である場合、または記録再生器制限情報が「する」で記録再生器識別子が不一致である場合は、処理を終了する。

【０５８１】

次に、ステップＳ７９３、Ｓ７９４、Ｓ７９５では、データ管理ファイルの記録データにしたがって復号鍵生成処理をステップＳ７９６～Ｓ７９９の４態様のいずれかに設定する。

【０５８２】

「プログラム使用制限あり」、かつ「記録再生器制限あり」の場合は、ステップＳ７９６において、コンテンツ固有鍵（ｅｘ．Ｋｃｏｎ）と、記録再生器固有鍵（Ｋｄｅｖ）の双方に基づいてセーブデータ復号化鍵Ｋｓａｖが生成される。または、別途、記録再生器３００の内部メモリ３０７内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ｋｓａｖとして使用してもよい。「プログラム使用制限あり」、かつ「記録再生器制限なし」の場合は、ステップＳ７９７において、コンテンツ固有鍵（ｅｘ．Ｋｃｏｎ）をセーブデータ復号化鍵Ｋｓａｖとするか、あるいはコンテンツ固有鍵（ｅｘ．Ｋｃｏｎ）に基づいてセーブデータ復号化鍵Ｋｓａｖを生成する。または、別途、記録再生器３００の内部メモリ３０７内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ｋｓａｖとして使用してもよい。

【０５８３】

「プログラム使用制限なし」、かつ「記録再生器制限あり」の場合は、ステッ

プＳ７９８において、記録再生器固有鍵（Ｋｄｅｖ）をセーブデータ復号化鍵Ｋｓａｖとするか、あるいは記録再生器固有鍵（Ｋｄｅｖ）に基づいてセーブデータ復号化鍵Ｋｓａｖが生成される。または、別途、記録再生器３００の内部メモリ３０７内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ｋｓａｖとして使用してもよい。さらに、「プログラム使用制限なし」、かつ「記録再生器制限なし」の場合は、ステップＳ７９９において、システム共通鍵、例えばシステム署名鍵Ｋｓｙｓをセーブデータ復号化鍵Ｋｓａｖとするか、あるいはシステム署名鍵Ｋｓｙｓに基づいてセーブデータ復号化鍵Ｋｓａｖを生成する。または、別途、記録再生器３００の内部メモリ３０７内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ｋｓａｖとして使用してもよい。

【０５８４】

これらの復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、同一のコンテンツ固有鍵、記録再生器固有鍵に基づいて暗号化されたデータは、同一のコンテンツ固有鍵、記録再生器固有鍵に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。

【０５８５】

ステップＳ８００では、上述のステップＳ７９６～Ｓ７９９のいずれかにおいて生成されたセーブデータ復号化鍵を用いて復号処理が実行され、復号セーブデータが記録再生器３００において再生、実行される。

【０５８６】

この図８０、８２において示したセーブデータ格納、再生処理フローによれば、「プログラム使用制限する」の選択がなされたセーブデータはコンテンツ固有鍵によって暗号化、復号化処理が実行されるため、同一のコンテンツ固有鍵を持つコンテンツデータを使用する場合のみ復号して利用することが可能となる。また、「記録再生器制限する」の選択がなされたセーブデータは、記録再生器識別子によって暗号化、復号化処理が実行されるため、同一の記録再生器識別子を持つ記録再生器、すなわち同一の記録再生器によってのみ復号して利用することが可能となる。従って、コンテンツ、記録再生器両者によって利用制限を設定することが可能となり、セーブデータのセキュリテイをさらに高めることが可能とな

る。

【０５８７】

なお、図８０、８２においては、コンテンツ固有鍵、記録再生器個有鍵を用いたセーブデータ暗号化鍵、復号化鍵の生成構成を示したが、コンテンツ個有鍵の代わりにコンテンツ識別子、また記録再生器固有鍵の代わりに記録再生器識別子を用いて、これら識別子に基づいてセーブデータ暗号化鍵、復号化鍵の生成を実行する構成としてもよい。

【０５８８】

次に、図８３～８５を用いてユーザの入力したパスワードに基づいてセーブデータの暗号化鍵、復号化鍵を生成する構成について説明する。

【０５８９】

図８３はユーザの入力したパスワードに基づいてセーブデータの暗号化鍵を生成して記録デバイスに格納する処理フローである。

【０５９０】

ステップＳ８２１は、コンテンツデータからコンテンツ識別子を読み出す処理であり、前述の各処理と同様である。ステップＳ８２２は、ユーザによるプログラム使用制限の設定を行なうか否かを決定するステップである。本構成において設定されるデータ管理ファイルは、例えば図８４に示す構成を持つ。

【０５９１】

図８４に示すように、データは、データ番号、コンテンツ識別子、記録再生器識別子、さらにユーザによるプログラム使用制限情報が含まれる。「ユーザによるプログラム使用制限情報」はプログラムを使用するユーザを制限するかしないかを設定する項目である。

【０５９２】

図８３における処理フローにおけるステップＳ８２２において使用制限するの設定がなされると、ステップＳ８２３においてユーザパスワードの入力がなされる。この入力は、図２に示す例えばキーボード等の入力手段から入力される。

【０５９３】

入力されたパスワードは、メインＣＰＵ１０６、制御部３０１の制御のもとに

暗号処理部３０２に出力され、ステップＳ８２４における処理、すなわち入力ユーザパスワードに基づくセーブデータ暗号化鍵Ｋｓａｖが生成される。セーブデータ暗号化鍵Ｋｓａｖ生成処理としては、例えばパスワード自体を暗号化鍵Ｋｓａｖとしてもよいし、あるいは記録再生器のマスタ鍵ＭＫｘを用いて、セーブデータ暗号化鍵Ｋｓａｖ＝ＤＥＳ（ＭＫｘ，パスワード）によって生成してもよい。また、パスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵を生成してもよい。

【０５９４】

ステップＳ８２２におけるユーザ制限がＮｏとされている場合は、ステップＳ８２８において、記録再生器３００のシステム共通鍵に基づいてセーブデータ暗号化鍵が生成される。

【０５９５】

さらに、ステップＳ８２５でステップＳ８２４、またはステップＳ８２８で生成したセーブデータ暗号化鍵Ｋｓａｖを用いてセーブデータの暗号化処理がなされ、ステップＳ８２６において暗号化処理のなされたセーブデータが記録デバイスに格納される。

【０５９６】

さらに、ステップＳ８２７において、図８４のデータ管理ファイルにステップＳ８２２で設定したユーザによるフログラム使用制限情報が、コンテンツ識別子と記録再生器識別子に対応付けられて書き込まれる。

【０５９７】

図８５は、図８３の処理によって格納されたセーブデータの再生処理フローを示した図である。ステップＳ８３１において、コンテンツデータからコンテンツ識別子を読み出し、ステップＳ８３２において図８４に示したデータ管理ファイルからコンテンツ識別子、ユーザによるプログラム使用制限情報を読み出す。

【０５９８】

ステップＳ８３３において、データ管理ファイル中のデータに基づく判定を実行し、「ユーザによるプログラム使用制限する」が設定されている場合は、ステップＳ８３４において、パスワード入力を求め、ステップＳ８３５において、入

力パスワードに基づく復号化鍵を生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、あるパスワードに基づいて暗号化されたデータは、同一のパスワードに基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムに設定される。

【０５９９】

ステップＳ８３３の判定がユーザによるプログラム使用制限なしの場合は、ステップＳ８３７において記録再生器３００の内部メモリに格納されたシステム共通鍵、例えばシステム署名鍵Ｋｓｙｓを用いてセーブデータ復号鍵Ｋｓａｖが生成される。または、別途、記録再生器３００の内部メモリ３０７内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ｋｓａｖとして使用してもよい。

【０６００】

ステップＳ８３６では、ステップＳ８３５、ステップＳ８３７のいずれかにおいて生成された復号化鍵Ｋｓａｖを用いて記録デバイスに格納されたセーブデータの復号が実行され、ステップＳ８３６において記録再生器においてセーブデータの再生、実行がなされる。

【０６０１】

図８３、図８５において示したセーブデータ格納、再生処理フローによれば、「ユーザによるプログラム使用制限する」の選択がなされたセーブデータはユーザ入力パスワードに基づく鍵によって暗号化、復号化処理が実行されるため、同一のパスワードを入力した場合のみ復号して利用することが可能とり、セーブデータのセキュリテイを高めることが可能となる。

【０６０２】

以上、いくつかのセーブデータの格納処理、再生処理態様について説明してきたが、上述した処理を融合した処理、例えばパスワードと、記録再生器識別子、コンテンツ識別子等を任意に組み合わせて使用してセーブデータ暗号化鍵、復号化鍵を生成する態様も可能である。

【０６０３】

（１７）不正機器の排除（リボケーション）構成

すでに説明してきたように、本発明のデータ処理装置においては、メディア５００（図３参照）、通信手段６００から提供される様々なコンテンツデータを記録再生器３００において、認証、暗号化処理等を実行し、記録デバイスに格納する構成によって提供コンテンツのセキュリティを高めるとともに、また、正当な利用者のみが利用可能とする構成を持つ。

【０６０４】

上述の説明から理解されるように、入力コンテンツは、記録再生器３００の暗号処理部３０２に構成される内部メモリ３０７に格納された様々な署名鍵、マスター鍵、チェック値生成鍵（図１８参照）を用いて、認証処理、暗号化処理、復号化処理がなされる。この鍵情報を格納する内部メモリ３０７は、先に説明したように、基本的に外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニュウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または／かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性とした構成とされるのが望ましいが、万が一内部メモリの不正な読み取りが実行され、これらの鍵データ等が流出し、正規なライセンスのされていない記録再生器にコピーされた場合、コピーされた鍵情報によって不正なコンテンツ利用がなされる可能性がある。

【０６０５】

ここでは、これらの不正コピーによる鍵の複製によるコンテンツの不正利用を防止する構成について説明する。

【０６０６】

図８６に、本構成「（１７）不正機器の排除構成」を説明するブロック図を示す。記録再生器３００は、前述の図２，３に示す記録再生器と同様であり、内部メモリを有し、先に説明した（図１８）各種の鍵データ、さらに、記録再生器識別子を有している。なお、ここでは、第三者によって複製されている記録再生器識別子、鍵データ等は図３に示す内部メモリ３０７に格納されるとは限らず、図８６に示す記録再生器３００の鍵データ等は、暗号処理部３０２（図２，３参照）によってアクセス可能なメモリ部にまとめて、あるいは分散して格納されている構成であるとする。

【０６０７】

不正機器の排除構成を実現するため、コンテンツデータのヘッダ部の不正な記録再生器識別子リストを記憶した構成とした。図８６に示すように、コンテンツデータには、不正な記録再生器識別子（ＩＤｄｅｖ）リストとしてのリボケーション(Revocation)リストを保有している。さらに、リボケーションリストの改竄チェック用のリストチェック値ＩＣＶｒｅｖを設けている。不正な記録再生器識別子（ＩＤｄｅｖ）リストは、コンテンツ提供者、または管理者が、例えば不正コピーの流通状態等から判明した不正な記録再生器の識別子ＩＤｄｅｖをリスト化したものである。このリボケーションリストは例えば配送鍵Ｋｄｉｓによって暗号化されて格納してもよい。記録再生器による復号処理については、例えば先の図２２のコンテンツダウンロード処理の態様と同様である。

【０６０８】

なお、ここでは、理解を容易にするため、リボケーションリストを単独のデータとして図８６のコンテンツデータ中に示してあるが、例えば先に説明したコンテンツデータのヘッダ部の構成要素である取扱方針（例えば図３２～３５参照）中にリボケーションリストを含ませてもよい。この場合は、先に説明したチェック値ＩＣＶａによってリボケーションリストを含む取扱方針データの改竄チェックがなされる。リボケーションリストが取扱方針中に含まれる場合は、チェック値Ａ：ＩＣＶａのチェックによって代替され、記録再生器内のチェック値Ａ生成鍵Ｋｉｃｖａが利用され、チェック値生成鍵Ｋｉｃｖ－ｒｅｖを格納する必要はない。

【０６０９】

リボケーションリストを単独のデータとしてコンテンツデータ中に含ませる場合は、リボケーションリストの改竄チェック用のリストチェック値ＩＣＶｒｅｖによるリボケーションリストのチェックを実行するとともに、リストチェック値ＩＣＶｒｅｖとコンテンツデータ中の他の部分チェック値とから中間チェック値を生成して中間チェック値の検証処理を行なう構成とする。

【０６１０】

リボケーションリストの改竄チェック用のリストチェック値ＩＣＶｒｅｖによ

るリボケーションリストのチェック手法は、前述の図２３、図２４等で説明したＩＣＶａ、ＩＣＶｂ等のチェック値生成処理と同様の方法で実行可能である。すなわち、記録再生器暗号処理部３０２の内部メモリ３０７に保存したチェック値生成鍵Ｋｉｃｖ－ｒｅｖを鍵とし、コンテンツデータ中に含まれるリボケーションリストをメッセージとして図２３、図２４等で説明したＩＣＶ計算方法に従って計算される。計算したチェック値ＩＣＶ－ｒｅｖ’とヘッダ（Header）内に格納されたチェック値：ＩＣＶ－ｒｅｖを比較し、一致していた場合には、改竄が無いと判定する。

【０６１１】

リストチェック値ＩＣＶｒｅｖを含む中間チェック値は、例えば、図２５に示すように、記録再生器暗号処理部３０２の内部メモリ３０７に保存されている総チェック値生成鍵Ｋｉｃｖｔを鍵とし、検証したHeader内のチェック値Ａ、チェック値Ｂ、リストチェック値ＩＣＶｒｅｖ、さらにフォーマットに応じてコンテンツチェック値を加えたメッセージ列に図７他で説明したＩＣＶ計算方法を適用して生成する。

【０６１２】

これらのリボケーションリスト、リストチェック値は、ＤＶＤ，ＣＤ等のメディア５００、通信手段６００を介して、あるいはメモリカード等の記録デバイス４００を介して記録再生器３００に提供される。ここで記録再生器３００は、正当な鍵データを保有する記録再生器である場合と、不正に複製された識別子ＩＤを有する場合とがある。

【０６１３】

このような構成における不正な記録再生器の排除処理の処理フローを図８７および図８８に示す。図８７は、ＤＶＤ，ＣＤ等のメディア５００、あるいは通信手段６００からコンテンツが提供される場合の不正記録再生器排除（リボケーション）処理フローであり、図８８は、メモリカード等の記録デバイス４００からコンテンツが提供される場合の不正記録再生器排除（リボケーション）処理フローである。

【０６１４】

まず、図８７の処理フローについて説明する。ステップ９０１は、メディアを装着して、コンテンツの提供、すなわち再生処理あるいはダウンロードの要求を行なうステップである。この図８７に示す処理は、例えば記録再生器にＤＶＤ等のメディアを装着してダウンロード処理等を実行する前のステップとして実行される。ダウンロード処理については、先に図２２を用いて説明している通りであり、図２２の処理フローの実行の前ステップとして、あるいは図２２の処理フロー中に挿入される処理としてこの図８７の処理が実行される。

【０６１５】

記録再生器３００がネットワーク等の通信手段を介してコンテンツ提供を受ける場合は、ステップＳ９１１においてコンテンツ配信サービス側との通信セッションを確立し、その後、ステップＳ９０２へ進む。

【０６１６】

ステップＳ９０２では、コンテンツデータのヘッダ部からリボケーションリスト(図８６参照)を取得する。このリスト取得処理は、コンテンツがメディア内にある場合は、図３に示す制御部３０１が読取部３０４を介してメデイアから読み出し、コンテンツが通信手段からである場合は、図３に示す制御部３０１が通信部３０５を介してコンテンツ配信側から受信する。

【０６１７】

次にステップＳ９０３において、制御部３０１は、暗号処理部３０２にメディア５００または通信手段６００から取得したリボケーションリストを暗号処理部３０２に渡し、チェック値生成処理を実行させる。記録再生器３００は、内部にリボケーションチェック値生成鍵Ｋｉｃｖ－ｒｅｖを有し、受領したリボケーションリストをメッセージとしてリボケーションチェック値生成鍵Ｋｉｃｖ－ｒｅｖを適用して、例えば図２３、図２４等で説明したＩＣＶ計算方法に従ってチェック値ＩＣＶ－ｒｅｖ’を計算し、計算結果とコンテンツデータのヘッダ（Header）内に格納されたチェック値：ＩＣＶ－ｒｅｖを比較し、一致していた場合には改竄が無い（ステップＳ９０４でＹｅｓ）と判定する。一致しない場合は、改竄されていると判定され、ステップＳ９０９に進み処理エラーとして処理を終了する。

【０６１８】

次に、ステップＳ９０５において、記録再生器暗号処理部３０２の制御部３０６は、記録再生器暗号処理部３０２の暗号／復号化部３０８に総チェック値ＩＣＶｔ’の計算をさせる。総チェック値ＩＣＶｔ’は、図２５に示すように、記録再生器暗号処理部３０２の内部メモリ３０７に保存されているシステム署名鍵Ｋｓｙｓを鍵とし、中間チェック値をＤＥＳで暗号化して生成する。なお、各部分チェック値、例えばＩＣＶａ、ＩＣＶｂ等の検証処理は、この図８７に示す処理フロー中では省略してあるが、先に説明した図３９～図４５の処理フローと同様の各データフォーマットに応じた部分チェック値の検証が行なわれる。

【０６１９】

次に、ステップＳ９０６において、生成した総チェック値ＩＣＶｔ’とヘッダ（Header）内のＩＣＶｔを比較し、一致していた場合（ステップＳ９０６でＹｅｓ）には、ステップＳ９０７へ進む。一致しない場合は、改竄されていると判定され、ステップＳ９０９に進み処理エラーとして処理を終了する。

【０６２０】

先に説明したように、総チェック値ＩＣＶｔは、ＩＣＶａ、ＩＣＶｂ、さらに、データフォーマットに応じて各コンテンツブロックのチェック値等、コンテンツデータに含まれる部分チェック値全体をチェックするものであるが、ここでは、これらの部分チェック値にさらに、リボケーションリストの改竄チェック用のリストチェック値ＩＣＶｒｅｖを部分チェック値として加えて、これら全ての改竄を検証する。上述の処理によって生成された総チェック値がヘッダ（Header）内に格納されたチェック値：ＩＣＶｔと一致した場合には、ＩＣＶａ、ＩＣＶｂ、各コンテンツブロックのチェック値、およびリストチェック値ＩＣＶｒｅｖ全ての改竄はないと判断される。

【０６２１】

さらにステップＳ９０７では、改竄無しと判定されたリボケーションリストと、自己の記録再生器３００に格納された記録再生器識別子（ＩＤｄｅｖ）との比較がなされる。

【０６２２】

コンテンツデータから読み出された不正な記録再生器識別子ＩＤｄｅｖのリストに自己の記録再生器の識別子ＩＤｄｅｖが含まれている場合は、その記録再生器３００は、不正に複製された鍵データを有していると判定され、ステップＳ９０９に進み、以後の手続きは中止される。例えば図２２のコンテンツダウンロード処理の手続きの実行を不可能とする。

【０６２３】

ステップＳ９０７において、不正な記録再生器識別子ＩＤｄｅｖのリストに自己の記録再生器の識別子ＩＤｄｅｖが含まれていないと判定された場合には、その記録再生器３００は、正当な鍵データを有していると判定され、ステップＳ９０８に進み、以後の手続き、例えば、プログラム実行処理、あるいは図２２等のコンテンツダウンロード処理等が実行可能となる。

【０６２４】

図８８は、メモリカード等の記録デバイス４００に格納したコンテンツデータを再生する場合の処理を示す。先に説明したように、メモリカード等の記録デバイス４００と記録再生器３００は、図２０で説明した相互認証処理（ステップＳ９２１）が実行される。ステップＳ９２２おいて、相互認証ＯＫである場合にのみ、ステップＳ９２３以降の処理に進み、相互認証に失敗した場合は、ステップＳ９３０のエラーとなり、以降の処理は実行されない。

【０６２５】

ステップＳ９２３では、コンテンツデータのヘッダ部からリボケーションリスト(図８６参照)を取得する。以降のステップＳ９２４～Ｓ９３０の処理は、先の図８７における対応処理と同様の処理である。すなわち、リストチェック値によるリストの検証（Ｓ９２４，Ｓ９２５）、総チェック値による検証（Ｓ９２６，Ｓ９２７）、リストのエントリと自己の記録再生器識別子ＩＤｄｅｖとの比較（Ｓ９２８）を実行し、コンテンツデータから読み出された不正な記録再生器識別子ＩＤｄｅｖのリストに自己の記録再生器の識別子ＩＤｄｅｖが含まれている場合は、その記録再生器３００は、不正に複製された鍵データを有していると判定され、ステップＳ９３０に進み、以後の手続きは中止される。例えば図２８に示すコンテンツの再生処理を実行不可能とする。一方、不正な記録再生器識別子Ｉ

Ｄｄｅｖのリストに自己の記録再生器の識別子ＩＤｄｅｖが含まれていないと判定された場合には、その記録再生器３００は、正当な鍵データを有していると判定され、ステップＳ９２９に進み、以後の手続きが実行可能となる。

【０６２６】

このように、本発明のデータ処理装置においては、コンテンツ提供者、または管理者が提供するコンテンツに併せて不正な記録再生器を識別するデータ、すなわち不正な記録再生器識別子ＩＤｄｅｖをリスト化したリボケーションリストをコンテンツデータのヘッダ部の構成データとして含ませて記録再生器利用者に提供し、記録再生器利用者は、記録再生器によるコンテンツの利用に先立って、自己の記録再生器のメモリに格納された記録再生器識別子ＩＤｄｅｖと、リストの識別子との照合を実行して一致するデータが存在した場合には、以後の処理を実行させない構成としたので鍵データを複製してメモリに格納した不正な記録再生器によるコンテンツ利用を排除することが可能となる。

【０６２７】

（１８）セキュアチップ構成および製造方法

先に説明したように、記録再生器暗号処理部３０２の内部メモリ３０７、あるいは記録デバイス４００の内部メモリ４０５は、暗号鍵などの重要な情報を保持しているため、外部から不正に読み出しにくい構造にしておく必要がある。従って、記録再生器暗号処理部３０２、記録デバイス暗号処理部４０１は、例えば外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニュウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または／かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性を有する耐タンパメモリとして構成される。

【０６２８】

しかしながら、上述の説明で理解されるように、例えば記録再生器暗号処理部３０２の内部メモリ３０７には記録再生器署名鍵Ｋｄｅｖ等の記録再生器毎に異なるデータを書き込むことが必要となる。また、チップ内の不揮発性の記憶領域、例えばフラッシュメモリ、ＦｅＲＡＭ等にチップ毎の個別情報、例えば識別情報（ＩＤ）や暗号鍵情報を書き込んだ後、例えば製品出荷後におけるデータの再

書き込み、読み出しを困難とすることが必要となる。

【０６２９】

従来の書き込みデータの読み出し、再書き込み処理を困難とするための手法には、例えばデータ書き込みのコマンドプロトコルを秘密にする。あるいは、チップ上のデータ書き込みコマンドを受け付ける信号線と、製品化した後に利用される通信用の信号線を分離して構成し、基板上のチップに直接信号を送らない限りデータ書き込みコマンドが有効とならないようにする等の手法がある。

【０６３０】

しかしながら、このような従来手法を採用しても、記憶素子の専門知識を有するものにとっては、回路を駆動させる設備と技術があれば、チップのデータ書き込み領域に対する信号出力が可能であり、また、たとえデータ書き込みのコマンドプロトコルが秘密であったとしても、プロトコルの解析可能性は常に存在する。

【０６３１】

このような、秘密データの改変可能性を保持した暗号処理データの格納素子を流通させることは、暗号処理システム全体を脅かす結果となる。また、データの読み出しを防止するために、データ読み出しコマンド自体を実装しない構成とすることも可能であるが、その場合、正規のデータ書き込みを実行した場合であっても、メモリに対するデータ書き込みが実際に行われたか否かを確認したり、書き込まれたデータが正確に書き込まれているか否かを判定することが不可能となり、不良なデータ書き込みの行われたチップが供給される可能性が発生する。

【０６３２】

これらの従来技術に鑑み、ここでは、、例えばフラッシュメモリ、ＦｅＲＡＭ等の不揮発性メモリに正確なデータ書き込みを可能とするとともに、データの読み出しを困難にするセキュアチップ構成およびセキュアチップ製造方法を提供する。

【０６３３】

図８９に、例えば、前述の記録再生器暗号処理部３０２または記録デバイス４００の暗号処理部４０１に適用可能なセキュリティチップ構成を示す。図８９（

Ａ）はチップの製造過程、すなわちデータの書き込み過程におけるセキュリティチップ構成を示し、図８９（Ｂ）は、データを書き込んだセキュリティチップを搭載した製品の構成例、例えば記録再生器３００、記録デバイス４００の例を示す。

【０６３４】

製造過程にあるセキュリティチップは、処理部８００１にモード指定用信号線８００３、および各種コマンド信号線８００４が接続され、処理部８００１は、モード指定用信号線８００３で設定されたモード、例えばデータ書き込みモードまたはデータ読み出しモードに応じて不揮発性メモリである記憶部８００２へのデータ書き込み処理、または記憶部８００２からのデータ読み出し処理を実行する。

【０６３５】

一方、図８９（Ｂ）のセキュリティチップ搭載製品においては、セキュリティチップと外部接続インタフェース、周辺機器、他の素子等とが汎用信号線で接続されるが、モード信号線８００３は、非接続状態とされる。具体的な処理は、例えばモード信号線８００３をグランド接続する、Ｖｃｃに釣り上げる、信号線をカットする、あるいは絶縁体樹脂で封印する等である。このような処理により、製品出荷後は、セキュリティチップのモード信号線に対するアクセスが困難になり、外部からチップのデータを読み出したり書き込みを行なったりすることの困難性を高めることができる。

【０６３６】

さらに、本構成のセキュリティチップ８０００は、データの記憶部８００２に対する書き込み処理、および記憶部８００２に書き込まれたデータの読み出し処理を困難にする構成を持ち、たとえ第三者がモード信号線８００３のアクセスに成功した場合であっても不正なデータ書き込み、読み出しを防止可能である。図９０に本構成を有するセキュリティチップにおけるデータ書き込みまたは読み出し処理フローを示す。

【０６３７】

ステップＳ９５１は、モード信号線８００３をデータ書き込みモードまたはデ

ータ読み出しモードに設定するステップである。

【０６３８】

ステップＳ９５２は、チップから認証用情報を取り出すステップである。本構成のセキュリティチップには、例えばワイヤ（Ｗｉｒｅ）、マスクＲＯＭ構成により、予めパスワード、暗号技術における認証処理用の鍵情報等、認証処理に必要な情報が格納される。ステップＳ９５２は、この認証情報を読み出して認証処理を実行する。例えば正規なデータ書き込み治具、データ読み出し装置を汎用信号線に接続して認証処理を実行した場合には、認証ＯＫ（ステップＳ９５３においてＹｅｓ）の結果が得られるが、不正なデータ書き込み治具、データ読み出し装置を汎用信号線に接続して認証処理を実行した場合には、認証に失敗（ステップＳ９５３においてＮｏ）し、その時点で処理が中止される。認証処理は、例えば先に説明した図１３の相互認証処理手続きに従って実行可能である。図８９に示す処理部８００１は、これらの認証処理を実行可能な構成を有する。これは、例えば先に説明した図２９に示す記録デバイス４００の暗号処理部４０１の制御部４０３に組み込まれたコマンドレジスタと同様の構成により実現可能である。例えば図８９のチップの処理部は、図２９に示す記録デバイス４００の暗号処理部４０１の制御部４０３に組み込まれたコマンドレジスタと同様の構成を持ち、各種コマンド信号線８００４に接続された機器から所定のコマンドＮｏが入力されると、対応する処理を実行し、認証処理シーケンスを実行することが可能となる。

【０６３９】

処理部８００１は認証処理において認証がなされた場合にのみ、データの書き込みコマンド、またはデータの読み出しコマンドを受け付けてデータの書き込み処理（ステップＳ９５５）、またはデータの読み出し処理（ステップＳ９５６）を実行する。

【０６４０】

このように本構成のセキュリティチップにおいては、データの書き込み時、読み出し時に認証処理を実行する構成としたので、正当な権利を持たない第三者によるセキュリティチップの記憶部からデータの読み出し、または記憶部へのデー

タ書き込みを防止することができる。

【０６４１】

次に、さらに、セキュリティの高い素子構成とした実施例を図９１に示す。この例では、セキュリティチップの記憶部８２００が２つの領域に分離され、一方はデータの読み書きが可能な読み出し書き込み併用領域(ＲＷ：ＲｅａｄＷｒｉｔｅ領域)８２０１であり、他方はデータの書き込みのみが可能な書き込み専用領域（ＷＯ：ＷｒｉｔｅＯｎｌｙ領域）８２０２である。

【０６４２】

この構成において、書き込み専用領域（ＷＯ：ＷｒｉｔｅＯｎｌｙ領域）８２０２には、暗号鍵データ、識別子データ等のセキュリテイ要請の高いデータを書き込み、一方セキュリティ度のさほど高くない、例えばチェック用のデータ等を読み出し書き込み併用領域(ＲＷ：ＲｅａｄＷｒｉｔｅ領域)８２０１に書き込む。

【０６４３】

処理部８００１は、読み出し書き込み併用領域(ＲＷ：ＲｅａｄＷｒｉｔｅ領域)８２０１からのデータ読み出し処理は、前述の図９０で説明した認証処理を伴うデータ読み出し処理を実行する。しかし、データ書き込み処理は、図９２のフローに従って実行する。

【０６４４】

図９２のステップＳ９６１は、モード信号線８００３を書き込みモードに設定するステップであり、ステップ９６２では、先の図９０で説明したと同様の認証処理を実行する。認証処理で認証がなされると、ステップＳ９６３に進み、コマンド信号線８００４を介して、書き込み専用（ＷＯ）領域８２０２にセキュリテイの高い鍵データ等の情報の書き込み、読み出し書き込み併用領域(ＲＷ：ＲｅａｄＷｒｉｔｅ領域)８２０１にセキュリティ度のさほど高くない、例えばチェック用データ書き込むコマンドを処理部８００１に対して出力する。

【０６４５】

ステップＳ９６４ではコマンドを受領した処理部８００１が、コマンドに応じたデータ書き込み処理をそれぞれ書き込み専用（ＷＯ）領域８２０２、読み出し

書き込み併用領域(ＲＷ：ＲｅａｄＷｒｉｔｅ領域)８２０１に対して実行する。

【０６４６】

また、書き込み専用（ＷＯ）領域８２０２に書き込まれたデータの検証処理フローを図９３に示す。

【０６４７】

図９３のステップＳ９７１は、処理部８００１において、書き込み専用（ＷＯ）領域８２０２に書き込まれたデータに基づく暗号処理を実行させる。これらの実行構成は、先の認証処理実行構成と同様、コマンドレジスタに格納された暗号処理シーケンスを順次実行する構成によって実現される。また、処理部８００１において実行される暗号処理アルゴリズムは特に限定されるものではなく、例えば先に説明したＤＥＳアルゴリズムを実行する構成とすることができる。

【０６４８】

次に、ステップＳ９７２で、セキュリティチップに接続された検証装置が処理部８００１から暗号処理結果を受信する。次に、ステップＳ９７３において、先に記憶部に書き込み処理を行なった正規な書き込みデータに対して処理部８００１において実行されたアルゴリズムと同様の暗号化処理を適用して得た結果と、処理部８００１からの暗号化結果とを比較する。

【０６４９】

比較した結果が同一であれば、書き込み専用（ＷＯ）領域８２０２に書き込まれたデータは正しいことが検証される。

【０６５０】

この構成では、認証処理が破られて読み出しコマンドが万が一実行可能となっても、データの読み出し可能領域は、読み出し書き込み併用領域(ＲＷ：ＲｅａｄＷｒｉｔｅ領域)８２０１に限定され、書き込み専用（ＷＯ）領域８２０２に書き込まれたデータの読み出しは、不可能であり、さらにセキュリティの高い構成となる。また、全く読み出しを不可能としたチップと異なり、読み出し書き込み併用領域(ＲＷ：ＲｅａｄＷｒｉｔｅ領域)８２０１が構成されているのでメモリアクセスの正否チェックが可能である。

【０６５１】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。また、上記した実施例ではコンテンツの記録、再生を可能な記録再生器を例にして説明してきたが、データ記録のみ、データ再生のみ可能な装置においても本発明の構成は適用可能なものであり、本発明はパーソナルコンピュータ、ゲーム機器、その他の各種データ処理装置一般において実施可能なものである。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０６５２】

【発明の効果】

上述したように、本発明のデータ処理システム、記録デバイス、およびデータ処理方法においては、記録デバイスにおける認証処理、および格納データの暗号処理等の各種処理を実行コマンド順を予め定めた設定シーケンスにしたがって実行するように構成した。すなわち、記録再生器から記録デバイスに対してコマンド番号を送信し、記録デバイスの制御部が予め定めたシーケンスにしたがったコマンド番号のみを受け付けて実行する構成とするとともに、設定シーケンスの認証処理コマンドを暗号処理コマンドに先行して実行するように設定したので、認証処理の済んだ記録再生器のみが記録デバイスに対するコンテンツの格納、または再生処理が実行でき、認証処理の済まない不正な機器によるコンテンツ利用が排除可能となる。

【０６５３】

さらに、本発明のデータ処理システム、記録デバイス、およびデータ処理方法によれば、認証処理の済んだことを示す認証フラグを設定し、認証フラグの設定された機器に対しては、暗号化データの格納処理、再生処理を実行可能としたので、格納処理、再生処理を繰り返し実行する場合、認証フラグが設定されている場合は、繰り返し認証処理を実行する必要がなく、効率的なデータ処理が可能となる。

【図面の簡単な説明】

【図１】

従来のデータ処理システムの構成を示す図である。

【図２】

本発明の適用されるデータ処理装置の構成を示す図である。

【図３】

本発明の適用されるデータ処理装置の構成を示す図である。

【図４】

メディア上、通信路上におけるコンテンツデータのデータフォーマットを示す図である。

【図５】

コンテンツデータ中のヘッダに含まれる取扱方針を示す図である。

【図６】

コンテンツデータ中のヘッダに含まれるブロック情報を示す図である。

【図７】

ＤＥＳを用いた電子署名生成方法を示す図である。

【図８】

トリプルＤＥＳを用いた電子署名生成方法を示す図である。

【図９】

トリプルＤＥＳの態様を説明する図である。

【図１０】

一部にトリプルＤＥＳを用いた電子署名生成方法を示す図である。

【図１１】

電子署名生成における処理フローを示す図である。

【図１２】

電子署名検証における処理フローを示す図である。

【図１３】

対称鍵暗号技術を用いた相互認証処理の処理シーケンスを説明する図である。

【図１４】

公開鍵証明書を説明する図である。

【図１５】

非対称鍵暗号技術を用いた相互認証処理の処理シーケンスを説明する図である。

【図１６】

楕円曲線暗号を用いた暗号化処理の処理フローを示す図である。

【図１７】

楕円曲線暗号を用いた復号化処理の処理フローを示す図である。

【図１８】

記録再生器上のデータ保持状況を示す図である。

【図１９】

記録デバイス上のデータ保持状況を示す図である。

【図２０】

記録再生器と記録デバイスとの相互認証処理フローを示す図である。

【図２１】

記録再生器のマスタ鍵と記録デバイスの対応鍵ブロックとの関係を示す図である。

【図２２】

コンテンツのダウンロード処理における処理フローを示す図である。

【図２３】

チェック値Ａ：ＩＣＶａの生成方法を説明する図である。

【図２４】

チェック値Ｂ：ＩＣＶｂの生成方法を説明する図である。

【図２５】

総チェック値、記録再生器固有チェック値の生成方法を説明する図である。

【図２６】

記録デバイスに保存されたコンテンツデータのフォーマット（利用制限情報＝０）を示す図である。

【図２７】

記録デバイスに保存されたコンテンツデータのフォーマット（利用制限情報＝

１）を示す図である。

【図２８】

コンテンツの再生処理における処理フローを示す図である。

【図２９】

記録デバイスにおけるコマンド実行方法について説明する図である。

【図３０】

記録デバイスにおけるコンテンツ格納処理におけるコマンド実行方法について説明する図である。

【図３１】

記録デバイスにおけるコンテンツ再生処理におけるコマンド実行方法について説明する図である。

【図３２】

コンテンツデータフォーマットのフォーマット・タイプ０の構成を説明する図である。

【図３３】

コンテンツデータフォーマットのフォーマット・タイプ１の構成を説明する図である。

【図３４】

コンテンツデータフォーマットのフォーマット・タイプ２の構成を説明する図である。

【図３５】

コンテンツデータフォーマットのフォーマット・タイプ３の構成を説明する図である。

【図３６】

フォーマット・タイプ０におけるコンテンツチェック値ＩＣＶｉの生成処理方法を説明する図である。

【図３７】

フォーマット・タイプ１におけるコンテンツチェック値ＩＣＶｉの生成処理方法を説明する図である。

【図３８】

フォーマット・タイプ２，３における総チェック値、記録再生器固有チェック値の生成処理方法を説明する図である。

【図３９】

フォーマット・タイプ０，１におけるコンテンツダウンロード処理の処理フローを示す図である。

【図４０】

フォーマット・タイプ２におけるコンテンツダウンロード処理の処理フローを示す図である。

【図４１】

フォーマット・タイプ３におけるコンテンツダウンロード処理の処理フローを示す図である。

【図４２】

フォーマット・タイプ０におけるコンテンツ再生処理の処理フローを示す図である。

【図４３】

フォーマット・タイプ１におけるコンテンツ再生処理の処理フローを示す図である。

【図４４】

フォーマット・タイプ２におけるコンテンツ再生処理の処理フローを示す図である。

【図４５】

フォーマット・タイプ３におけるコンテンツ再生処理の処理フローを示す図である。

【図４６】

コンテンツ生成者と、コンテンツ検証者におけるチェック値の生成、検証方法を説明する図(その１)である。

【図４７】

コンテンツ生成者と、コンテンツ検証者におけるチェック値の生成、検証方法

を説明する図（その２）である。

【図４８】

コンテンツ生成者と、コンテンツ検証者におけるチェック値の生成、検証方法を説明する図（その３）である。

【図４９】

マスタ鍵を用いて各種の鍵を個別に生成する方法について説明する図である。

【図５０】

マスタ鍵を用いて各種の鍵を個別に生成する方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図（例１）である。

【図５１】

マスタ鍵を用いて各種の鍵を個別に生成する方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図（例２）である。

【図５２】

マスタ鍵の使い分けにより、利用制限を実行する構成について説明する図である。

【図５３】

マスタ鍵を用いて各種の鍵を個別に生成する方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図（例３）である。

【図５４】

マスタ鍵を用いて各種の鍵を個別に生成する方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図（例４）である。

【図５５】

マスタ鍵を用いて各種の鍵を個別に生成する方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図（例５）である。

【図５６】

トリプルＤＥＳを適用した暗号鍵をシングルＤＥＳアルゴリズムを用いて格納する処理フローを示す図である。

【図５７】

優先順位に基づくコンテンツ再生処理フロー（例１）を示す図である。

【図５８】

優先順位に基づくコンテンツ再生処理フロー（例２）を示す図である。

【図５９】

優先順位に基づくコンテンツ再生処理フロー（例３）を示す図である。

【図６０】

コンテンツ再生処理における圧縮データの復号（伸長）処理を実行する構成について説明する図である。

【図６１】

コンテンツの構成例（例１）を示す図である。

【図６２】

コンテンツの構成例１における再生処理フローを示す図である。

【図６３】

コンテンツの構成例（例２）を示す図である。

【図６４】

コンテンツの構成例２における再生処理フローを示す図である。

【図６５】

コンテンツの構成例（例３）を示す図である。

【図６６】

コンテンツの構成例３における再生処理フローを示す図である。

【図６７】

コンテンツの構成例（例４）を示す図である。

【図６８】

コンテンツの構成例４における再生処理フローを示す図である。

【図６９】

セーブデータの生成、格納処理について説明する図である。

【図７０】

セーブデータの格納処理例(例１)に関する処理フローを示す図である。

【図７１】

セーブデータの格納、再生処理において使用されるデータ管理ファイル構成（

例１）を示す図である。

【図７２】

セーブデータの再生処理例(例１)に関する処理フローを示す図である。

【図７３】

セーブデータの格納処理例(例２)に関する処理フローを示す図である。

【図７４】

セーブデータの再生処理例(例２)に関する処理フローを示す図である。

【図７５】

セーブデータの格納処理例(例３)に関する処理フローを示す図である。

【図７６】

セーブデータの格納、再生処理において使用されるデータ管理ファイル構成（例２）を示す図である。

【図７７】

セーブデータの再生処理例(例３)に関する処理フローを示す図である。

【図７８】

セーブデータの格納処理例(例４)に関する処理フローを示す図である。

【図７９】

セーブデータの再生処理例(例４)に関する処理フローを示す図である。

【図８０】

セーブデータの格納処理例(例５)に関する処理フローを示す図である。

【図８１】

セーブデータの格納、再生処理において使用されるデータ管理ファイル構成（例３）を示す図である。

【図８２】

セーブデータの再生処理例(例５)に関する処理フローを示す図である。

【図８３】

セーブデータの格納処理例(例６)に関する処理フローを示す図である。

【図８４】

セーブデータの格納、再生処理において使用されるデータ管理ファイル構成（

例４）を示す図である。

【図８５】

セーブデータの再生処理例(例６)に関する処理フローを示す図である。

【図８６】

コンテンツ不正利用者排除（リボケーション）構成を説明する図である。

【図８７】

コンテンツ不正利用者排除（リボケーション）の処理フロー（例１）を示す図である。

【図８８】

コンテンツ不正利用者排除（リボケーション）の処理フロー（例２）を示す図である。

【図８９】

セキュリティチップの構成（例１）を説明する図である。

【図９０】

セキュリティチップの製造方法における処理フローを示す図である。

【図９１】

セキュリティチップの構成（例２）を説明する図である。

【図９２】

セキュリティチップ（例２）におけるデータ書き込み処理における処理フローを示す図である。

【図９３】

セキュリティチップ（例２）における書き込みデータチェック処理における処理フローを示す図である。

【符号の説明】

１０６　メインＣＰＵ

１０７　ＲＡＭ

１０８　ＲＯＭ

１０９　ＡＶ処理部

１１０　入力処理部

１１１　ＰＩＯ

１１２　ＳＩＯ

３００　記録再生器

３０１　制御部

３０２　暗号処理部

３０３　記録デバイスコントローラ

３０４　読み取り部

３０５　通信部

３０６　制御部

３０７　内部メモリ

３０８　暗号／復号化部

４００　記録デバイス

４０１　暗号処理部

４０２　外部メモリ

４０３　制御部

４０４　通信部

４０５　内部メモリ

４０６　暗号／復号化部

４０７　外部メモリ制御部

５００　メディア

６００　通信手段

２１０１，２１０２，２１０３　記録再生器

２１０４，２１０５，２１０６　記録デバイス

２９０１　コマンド番号管理部

２９０２　コマンドレジスタ

２９０３，２９０４　認証フラグ

３００１　スピーカ

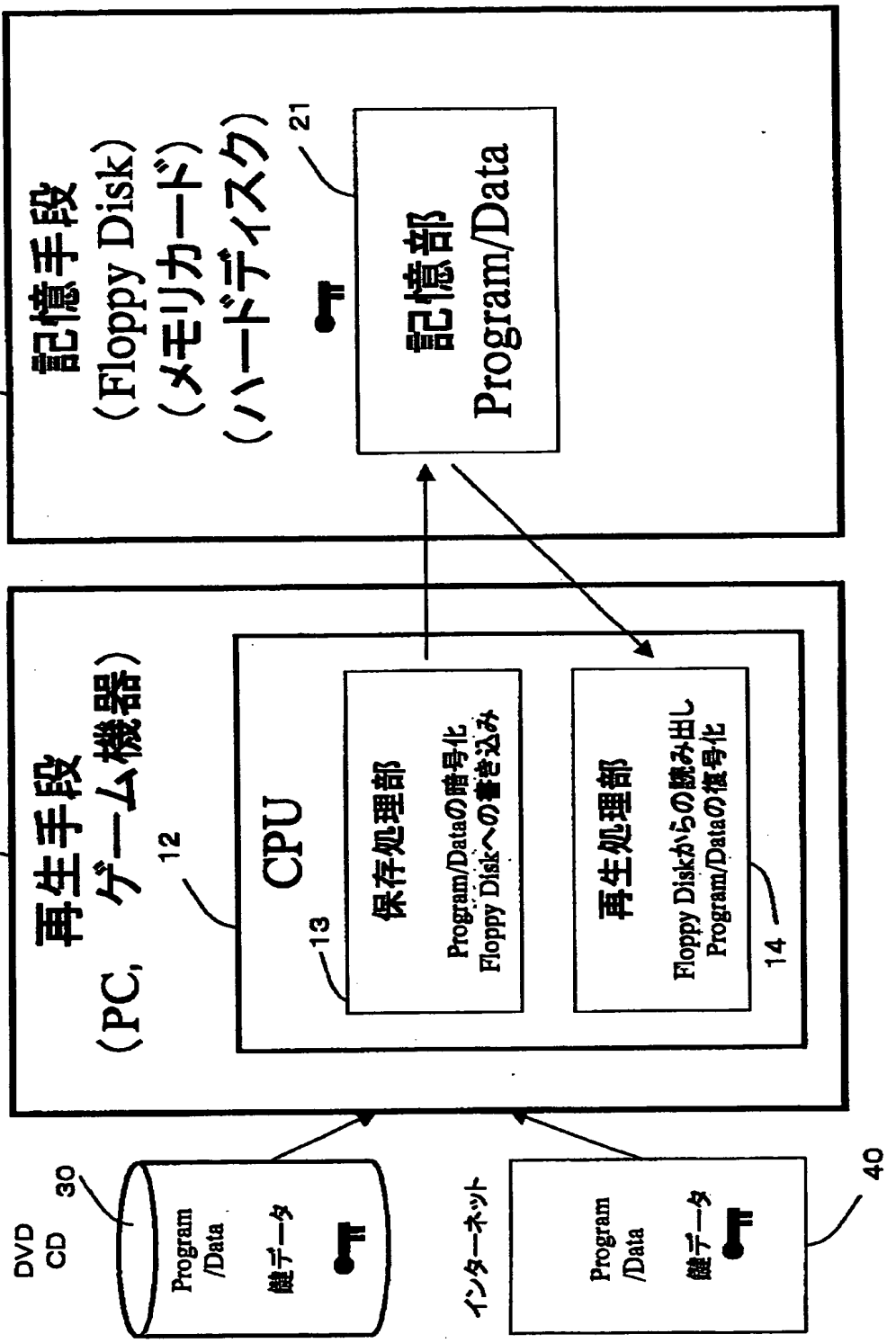
３００２　モニタ

３０９０　メモリ

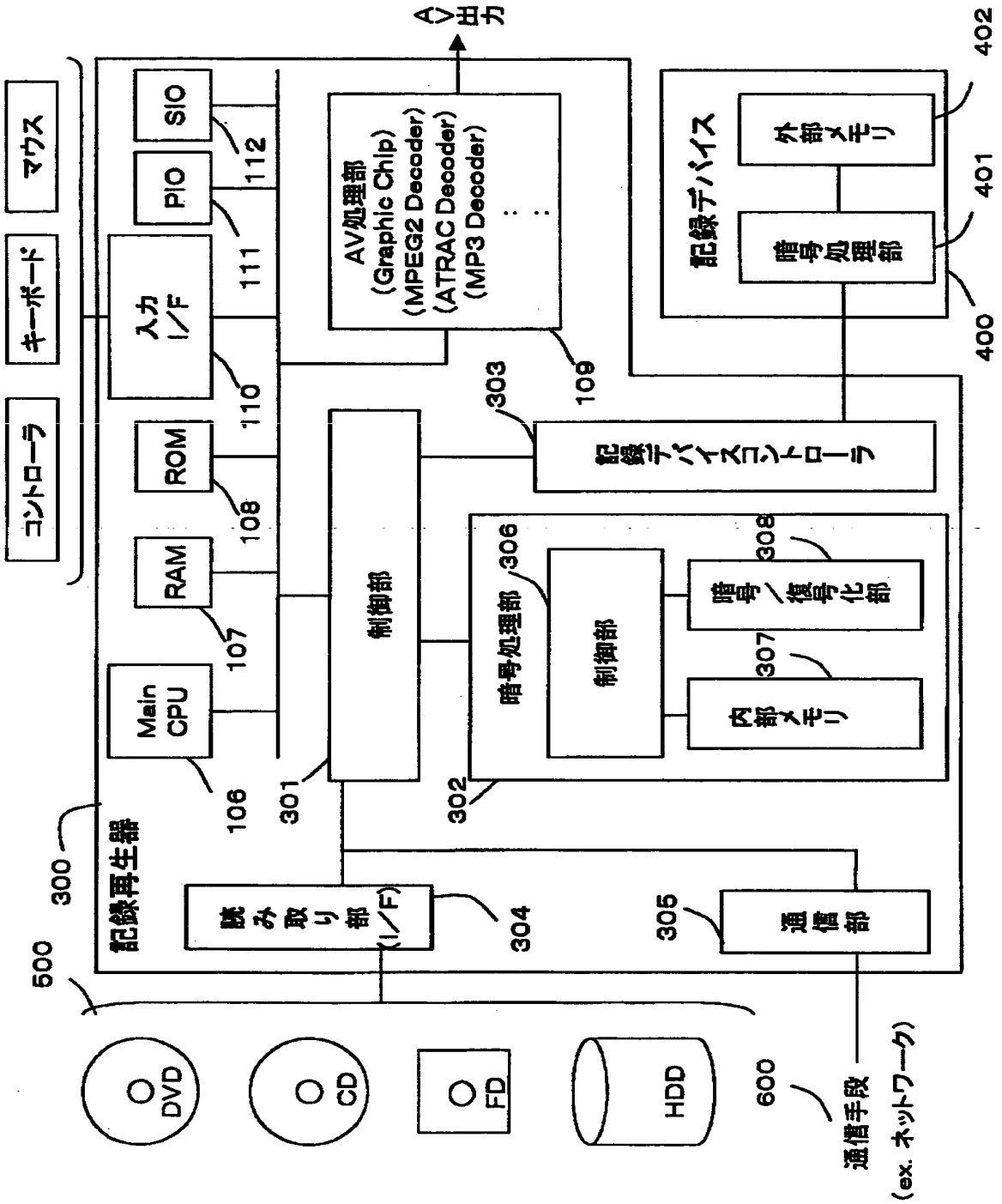
３０９１　コンテンツ解析部
３０９２　データ記憶部
３０９３　プログラム記憶部
３０９４　圧縮伸長処理部
７７０１　コンテンツデータ
７７０２　リボケーションリスト
７７０３　リストチェック値
８０００　セキュリティチップ
８００１　処理部
８００２　記憶部
８００３　モード信号線
８００４　コマンド信号線
８２０１　読み出し書き込み併用領域
８２０２　書き込み専用領域

【書類名】　　図面

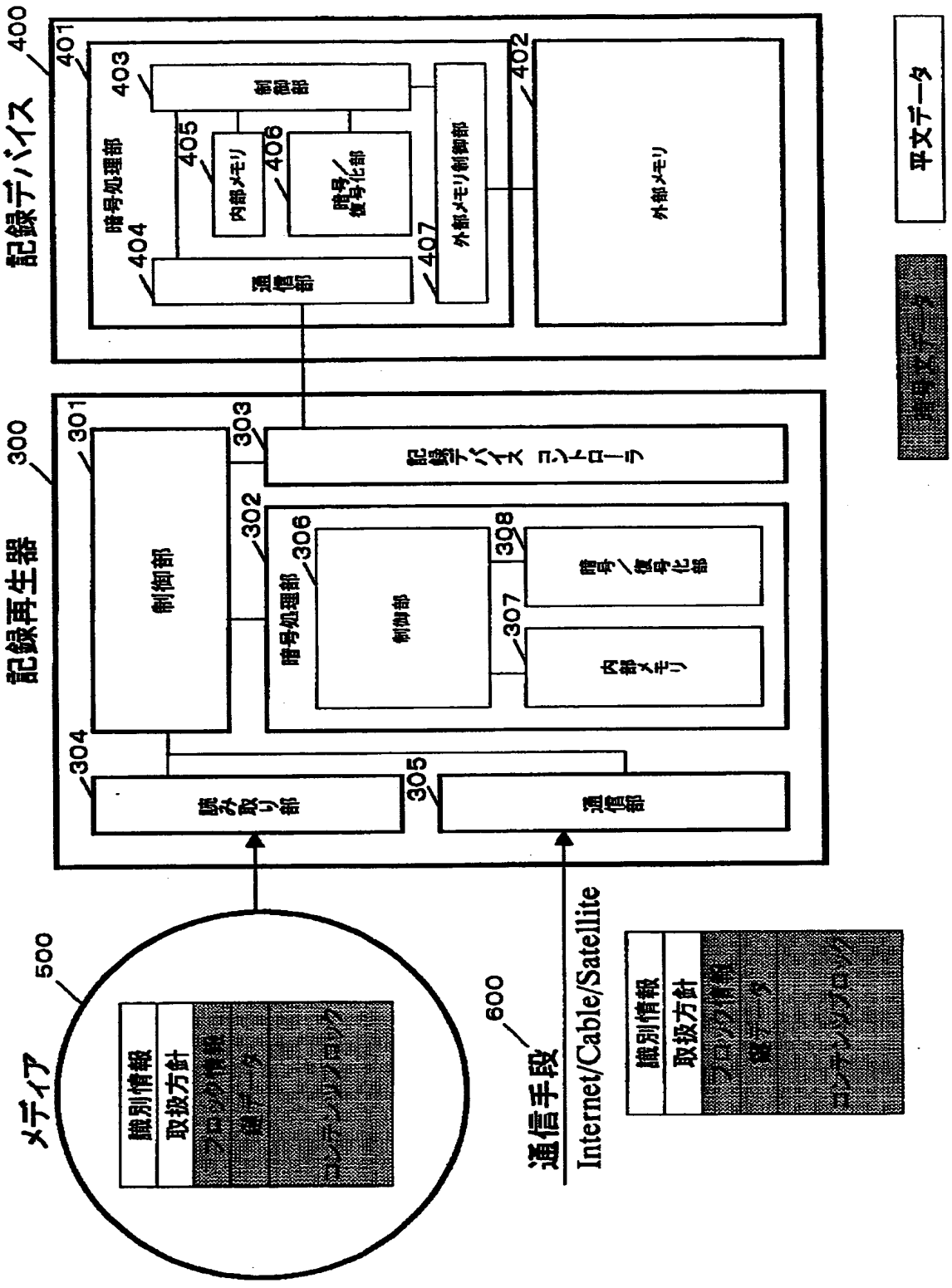
【図１】


記憶手段
(Floppy Disk)
(メモリカード)
(ハードディスク)
20
21
記憶部
Program/Data
再生手段
(PC, ゲーム機器)
10
12
CPU
13
保存処理部
Program/Dataの暗号化
Floppy Diskへの書き込み
再生処理部
Floppy Diskからの読み出し
Program/Dataの復号化
14
DVD
CD
30
Program
/Data
鍵データ
インターネット
Program
/Data
鍵データ
40

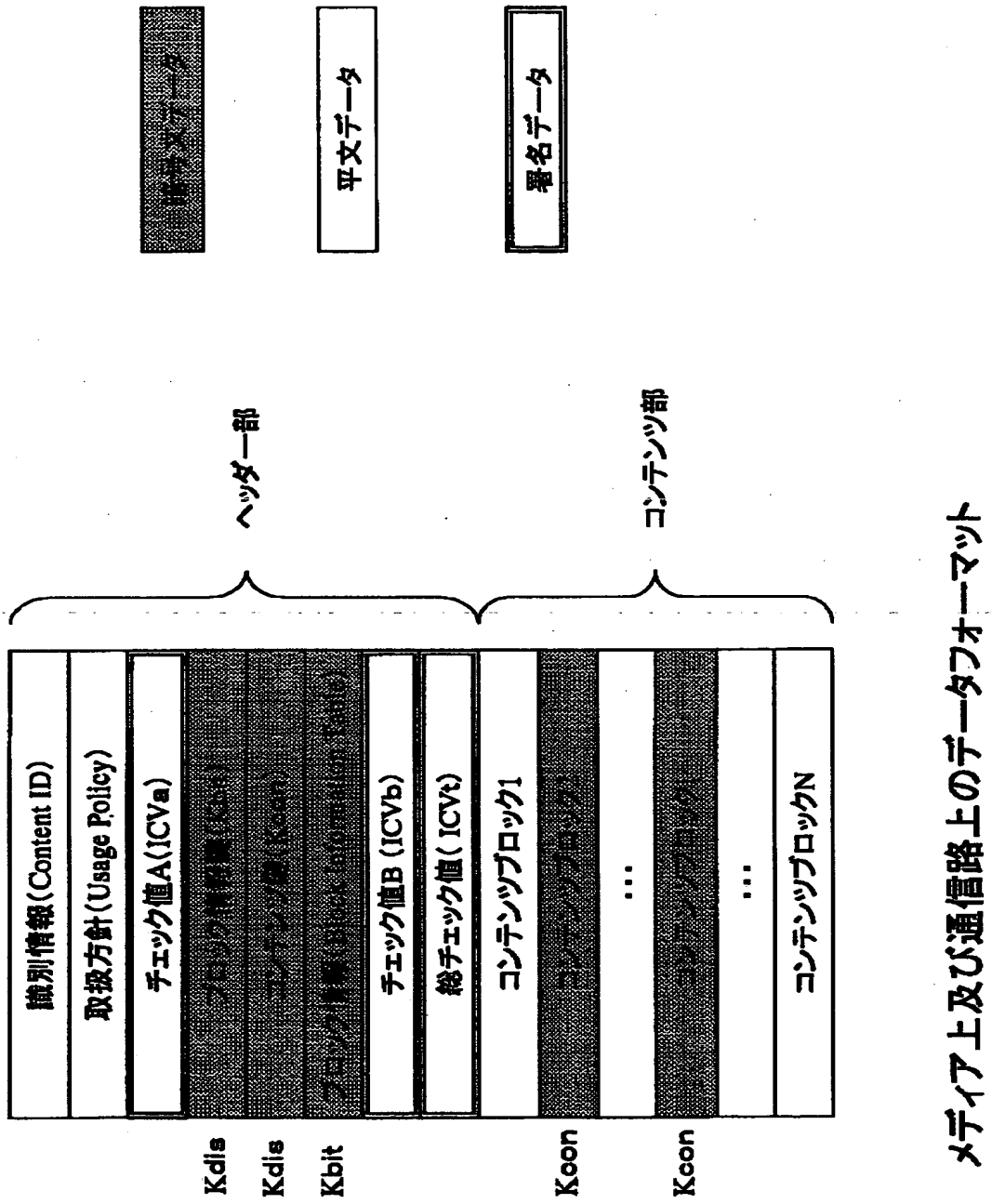
【図２】


A/V出力
マウス
キーボード
コントローラ
SIO
PIO
入力 I/F
ROM
RAM
Main CPU
112
111
110
108
107
106
AV処理部
(Graphic Chip)
(MPEG2 Decoder)
(ATRAC Decoder)
(MP3 Decoder)
109
制御部
301
記録デバイスコントローラ
303
暗号処理部
306
制御部
暗号／復号化部
308
内部メモリ
307
302
記録デバイス
外部メモリ
信号処理部
402
401
400
記録再生器
300
読み取り部 (I/F)
304
305
通信部
500
DVD
CD
FD
HDD
600
通信手段
(ex. ネットワーク)

【図３】


記録デバイス
400
401
暗号処理部
403
404
405
内部メモリ
406
暗号/復号化部
407
外部メモリ制御部
402
外部メモリ
記録再生器
300
301
制御部
303
302
306
制御部
308
307
内部メモリ
304
305
メディア
500
識別情報
取扱方針
通信手段
600
Internet/Cable/Satellite
識別情報
取扱方針
平文データ

【図４】



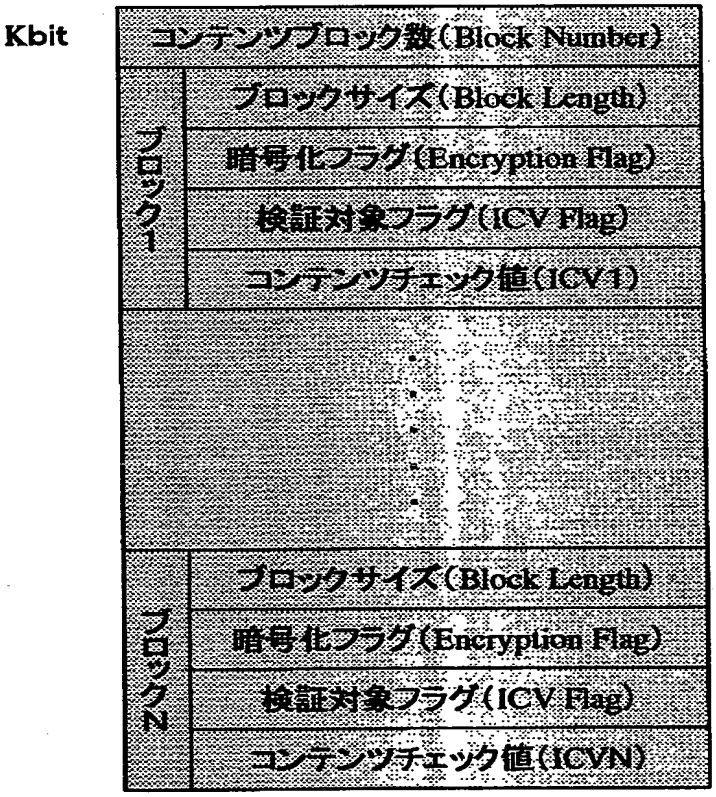
メディア上及び通信路上のデータフォーマット

【図５】

ヘッダーサイズ(Header Length)
コンテンツサイズ(Content Length)
フォーマットバージョン(Format Version)
フォーマットタイプ(Format Type)
コンテンツタイプ(Content Type)
起動優先順位情報(Operation Priority)
利用制限情報(Localization Field)
複製制限情報(Copy Permission)
移動制限情報(Move Permission)
暗号アルゴリズム(Encryption Algorithm)
暗号化モード(Encryption Mode)
検証方法(Integrity Check Method)

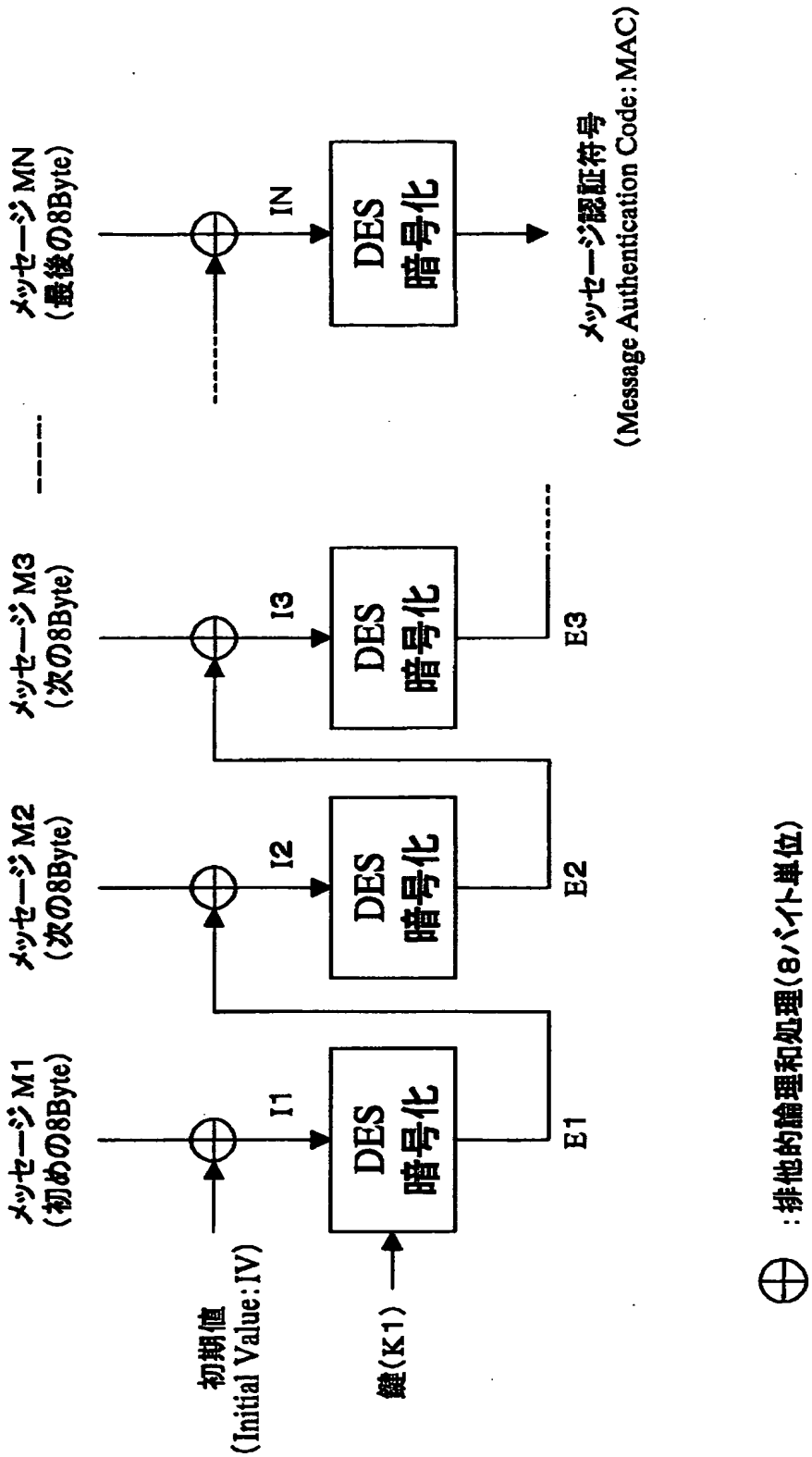
取扱方針

【図６】

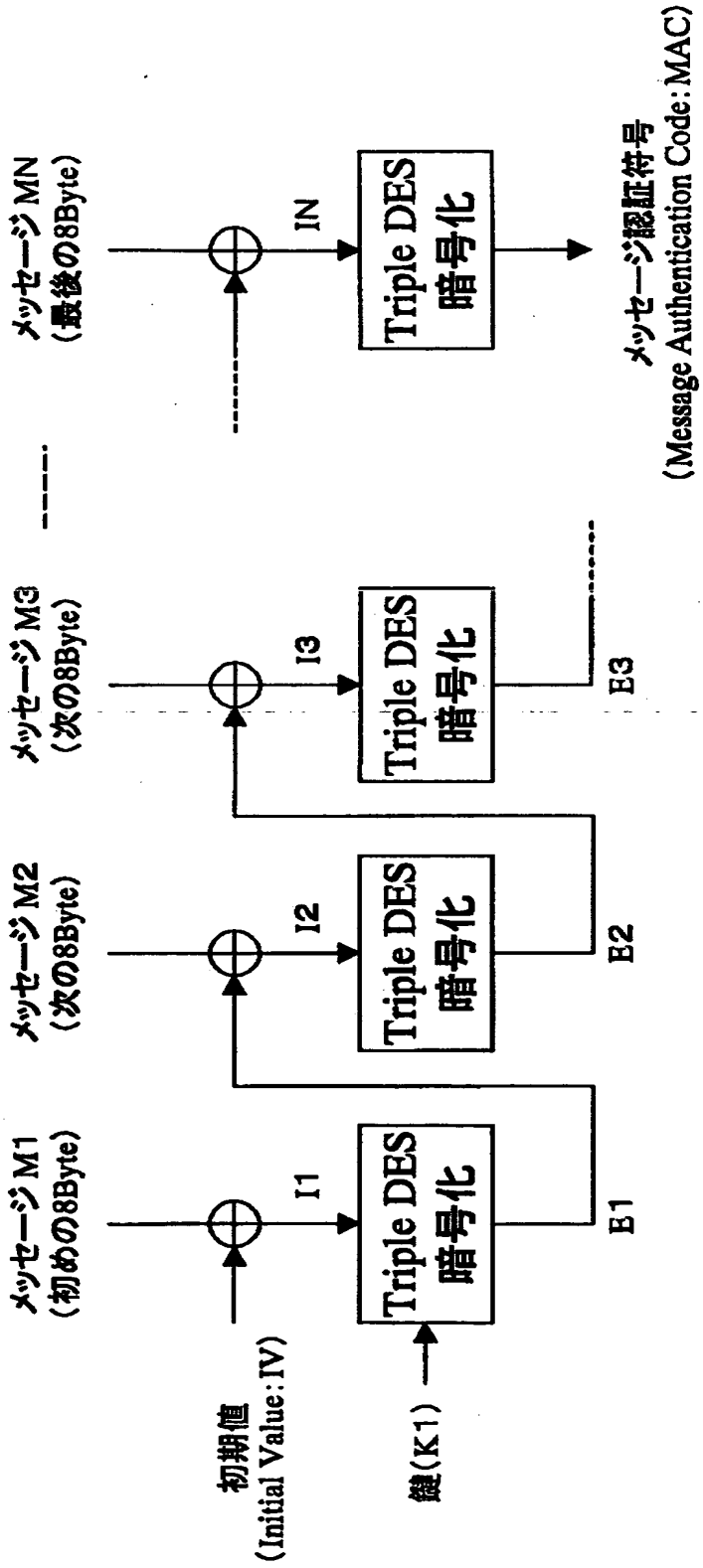

Kbit
コンテンツブロック数(Block Number)
ブロック1
ブロックサイズ(Block Length)
暗号化フラグ(Encryption Flag)
検証対象フラグ(ICV Flag)
コンテンツチェック値(ICV1)
ブロックN
ブロックサイズ(Block Length)
暗号化フラグ(Encryption Flag)
検証対象フラグ(ICV Flag)
コンテンツチェック値(ICVN)

ブロック情報

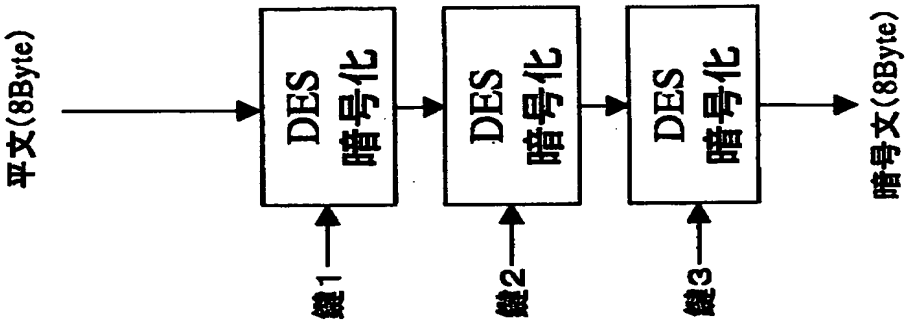
【図７】


メッセージ M1
(初めの8Byte)
メッセージ M2
(次の8Byte)
メッセージ M3
(次の8Byte)
メッセージ MN
(最後の8Byte)
I1
I2
I3
IN
DES
暗号化
E1
E2
E3
初期値
(Initial Value:IV)
鍵(K1)
メッセージ認証符号
(Message Authentication Code: MAC)
⊕ :排他的論理和処理(8バイト単位)

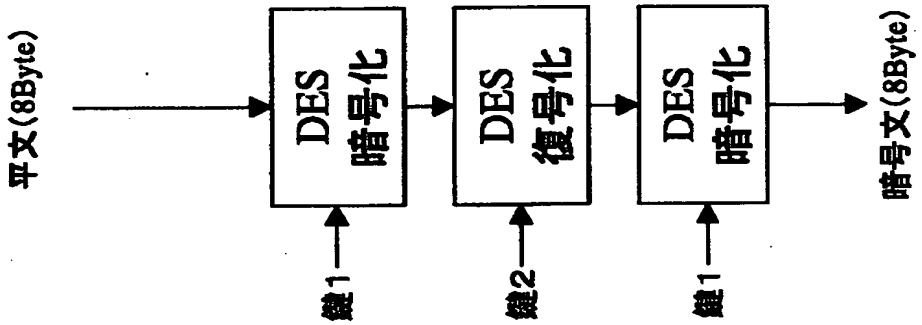
【図８】


メッセージ M1
(初めの8Byte)
メッセージ M2
(次の8Byte)
メッセージ M3
(次の8Byte)
メッセージ MN
(最後の8Byte)
初期値
(Initial Value:IV)
鍵(K1)
I1
I2
I3
IN
Triple DES
暗号化
E1
E2
E3
メッセージ認証符号
(Message Authentication Code:MAC)

【図９】

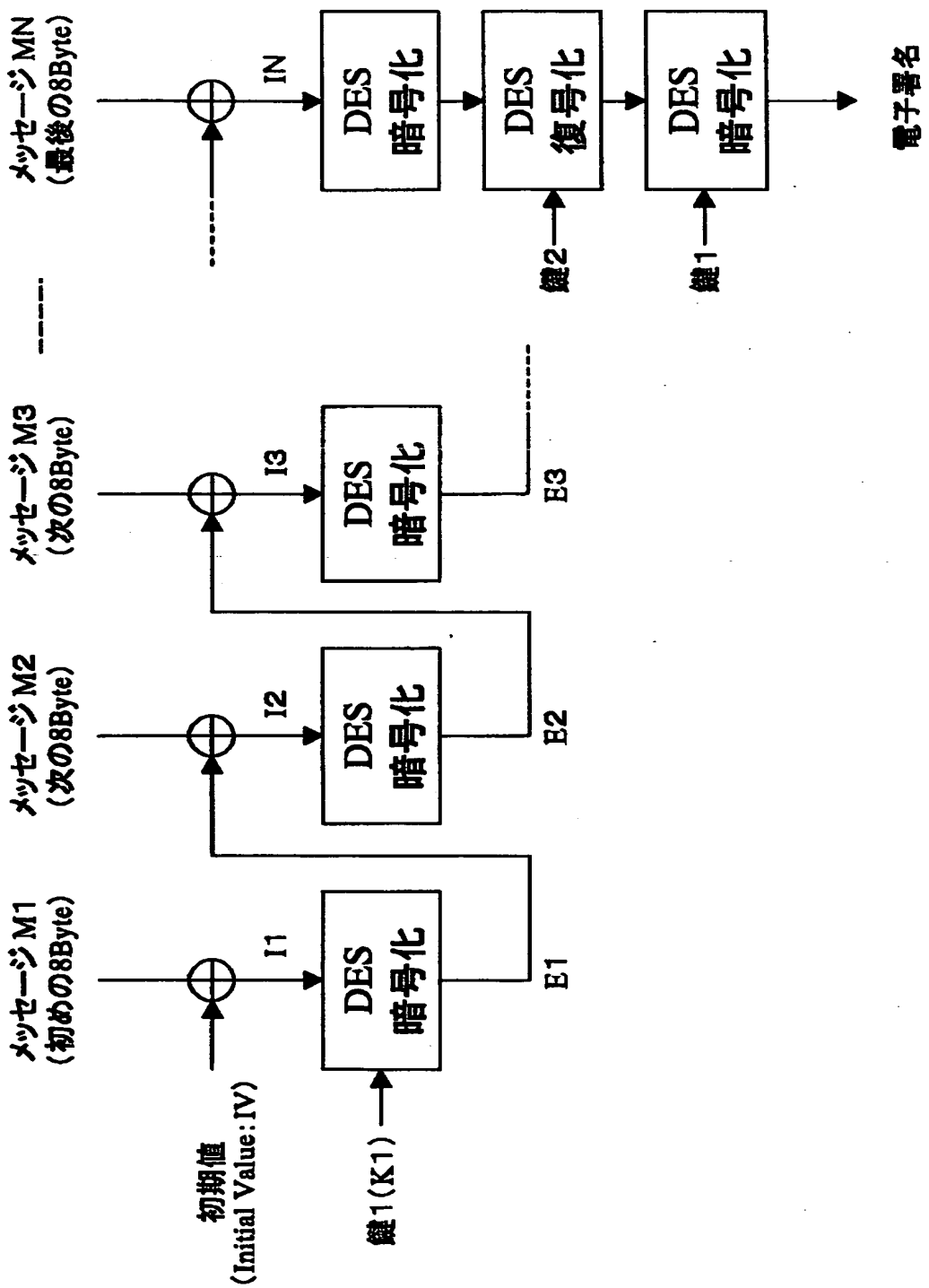

平文(8Byte)
DES 暗号化
DES 暗号化
DES 暗号化
暗号文(8Byte)
鍵1
鍵2
鍵3

(b)

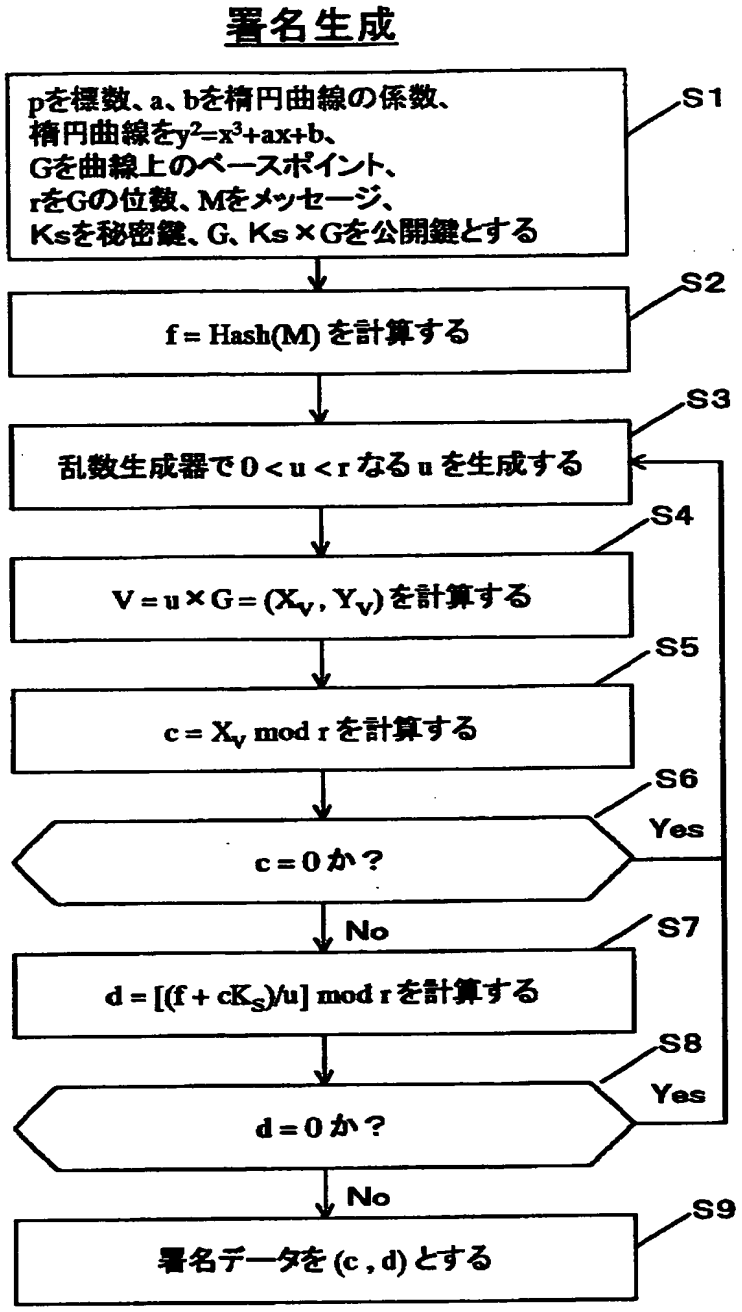

平文(8Byte)
DES 暗号化
DES 復号化
DES 暗号化
暗号文(8Byte)
鍵1
鍵2
鍵1

(a)

【図１０】

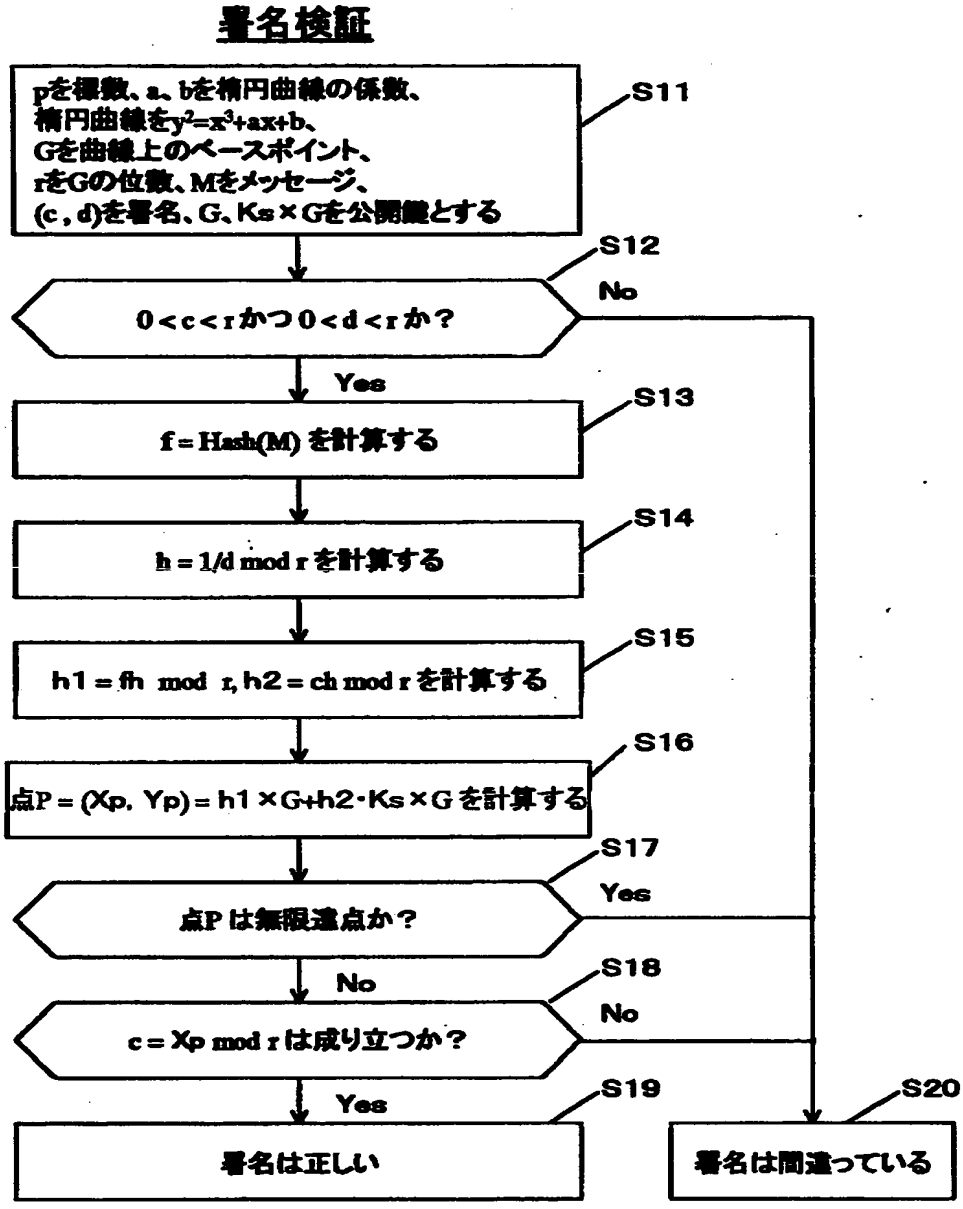

メッセージM1
(初めの8Byte)
メッセージM2
(次の8Byte)
メッセージM3
(次の8Byte)
メッセージMN
(最後の8Byte)
初期値
(Initial Value:IV)
I1
I2
I3
IN
DES
暗号化
DES
復号化
DES
暗号化
E1
E2
E3
鍵1(K1)
鍵2
鍵1
電子署名

【図１１】



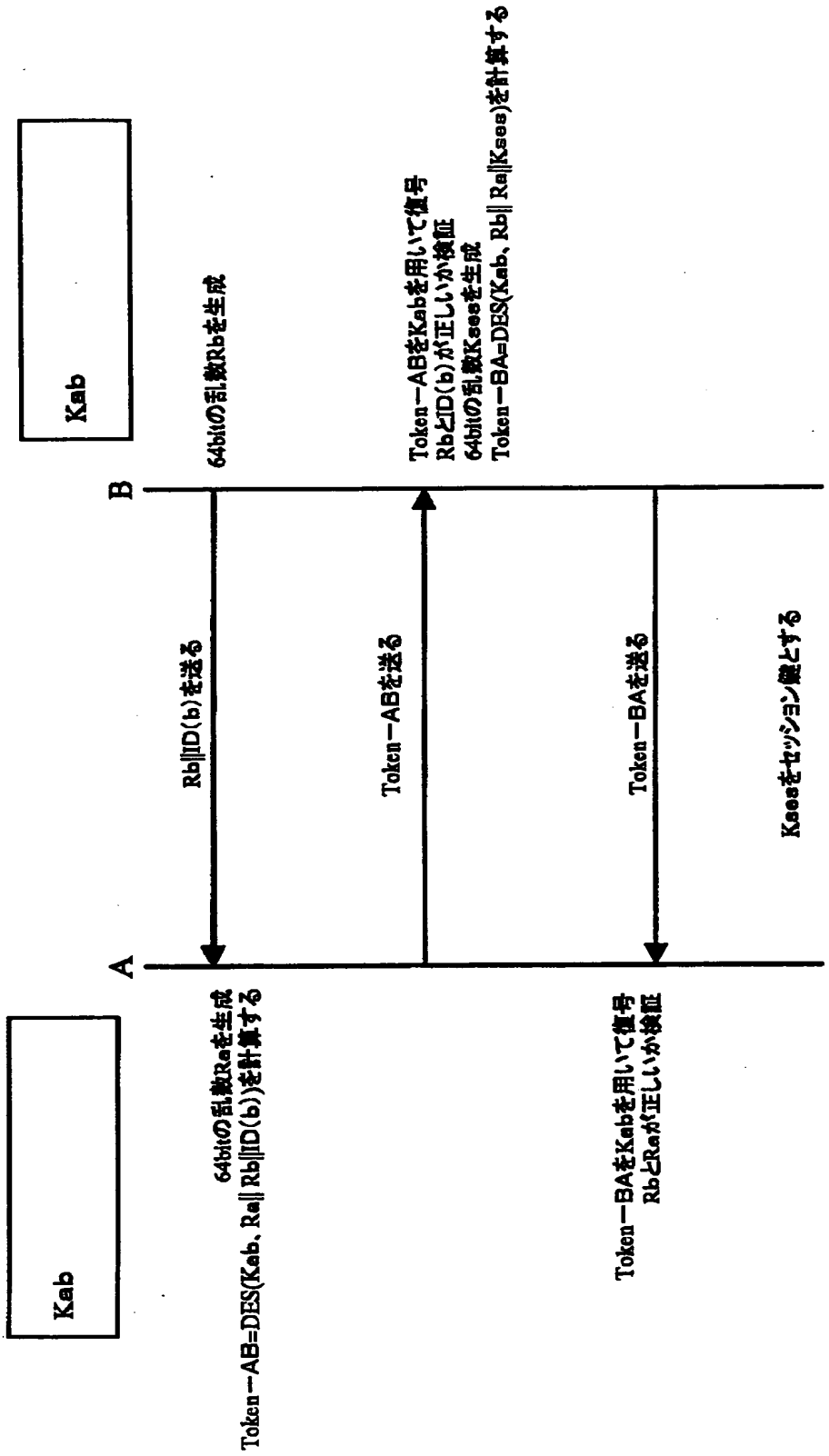
署名生成（IEEE P1363/D3）

【図１２】



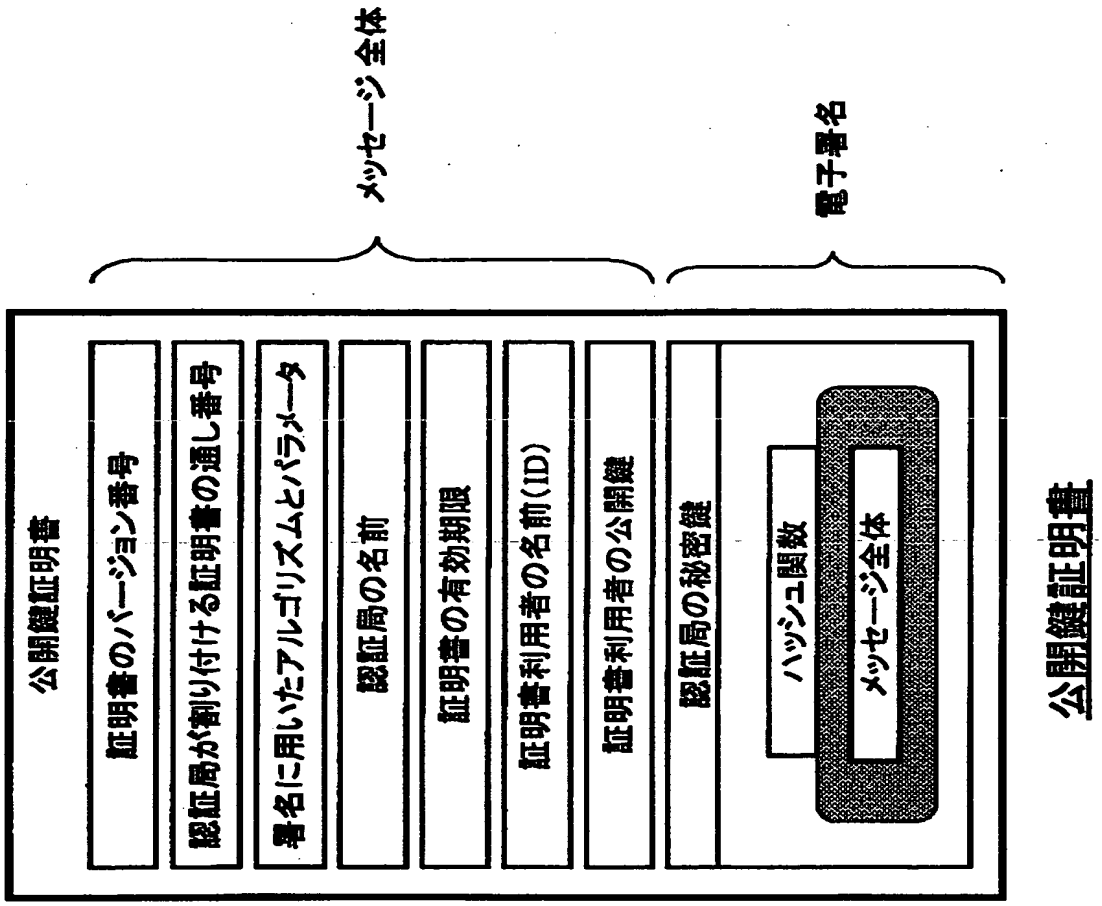
署名検証(IEEE P1363/D3)

【図１３】

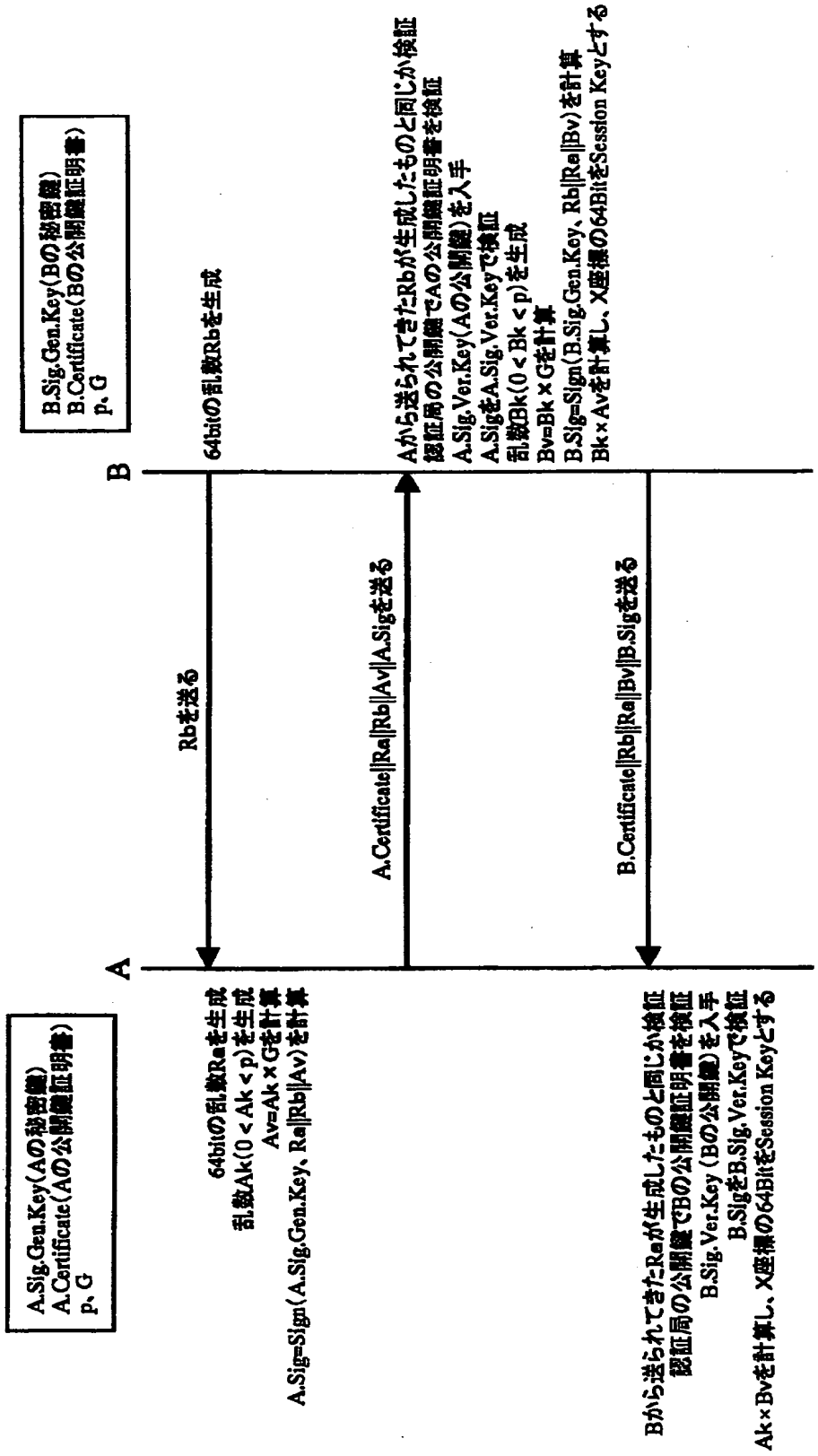


ISO/IEC 9798-2 対称鍵暗号技術を用いた相互認証および鍵共有方式

【図１４】

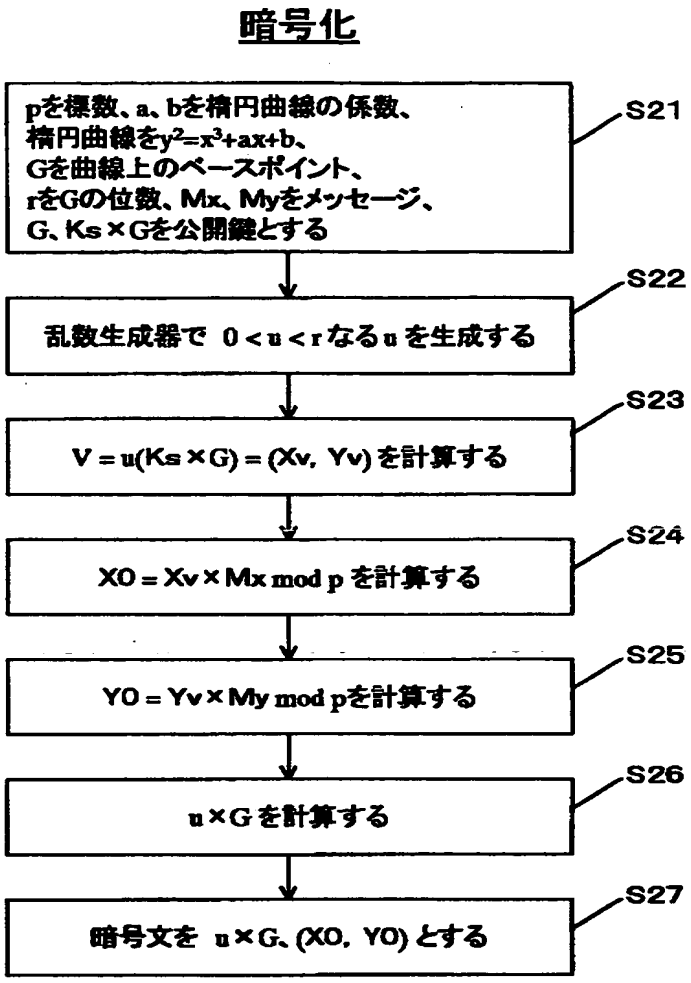

メッセージ全体
電子署名
公開鍵証明書
公開鍵証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
証明書利用者の名前(ID)
証明書利用者の公開鍵
認証局の秘密鍵
ハッシュ関数
メッセージ全体

【図１５】



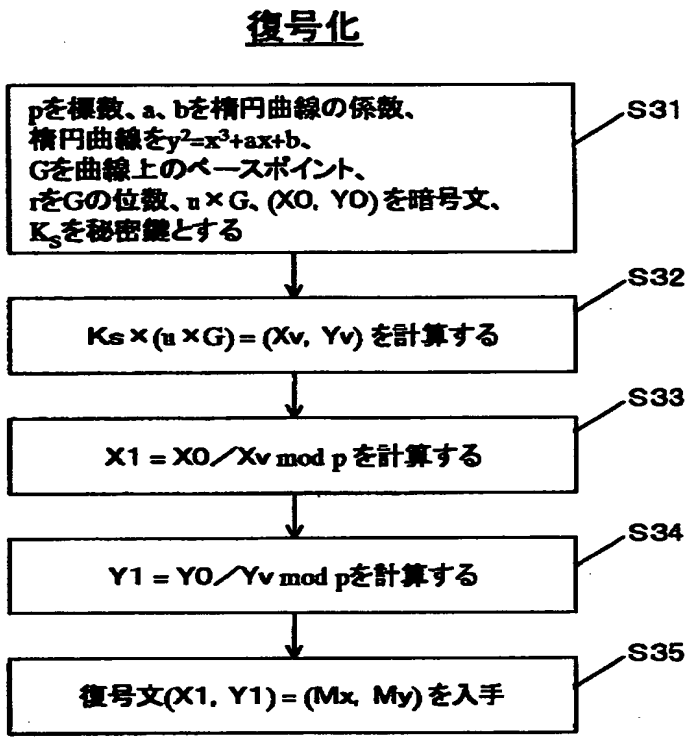
ISO/IEC 9798-3　非対称鍵暗号技術を用いた相互認証および鍵共有方式

【図１６】



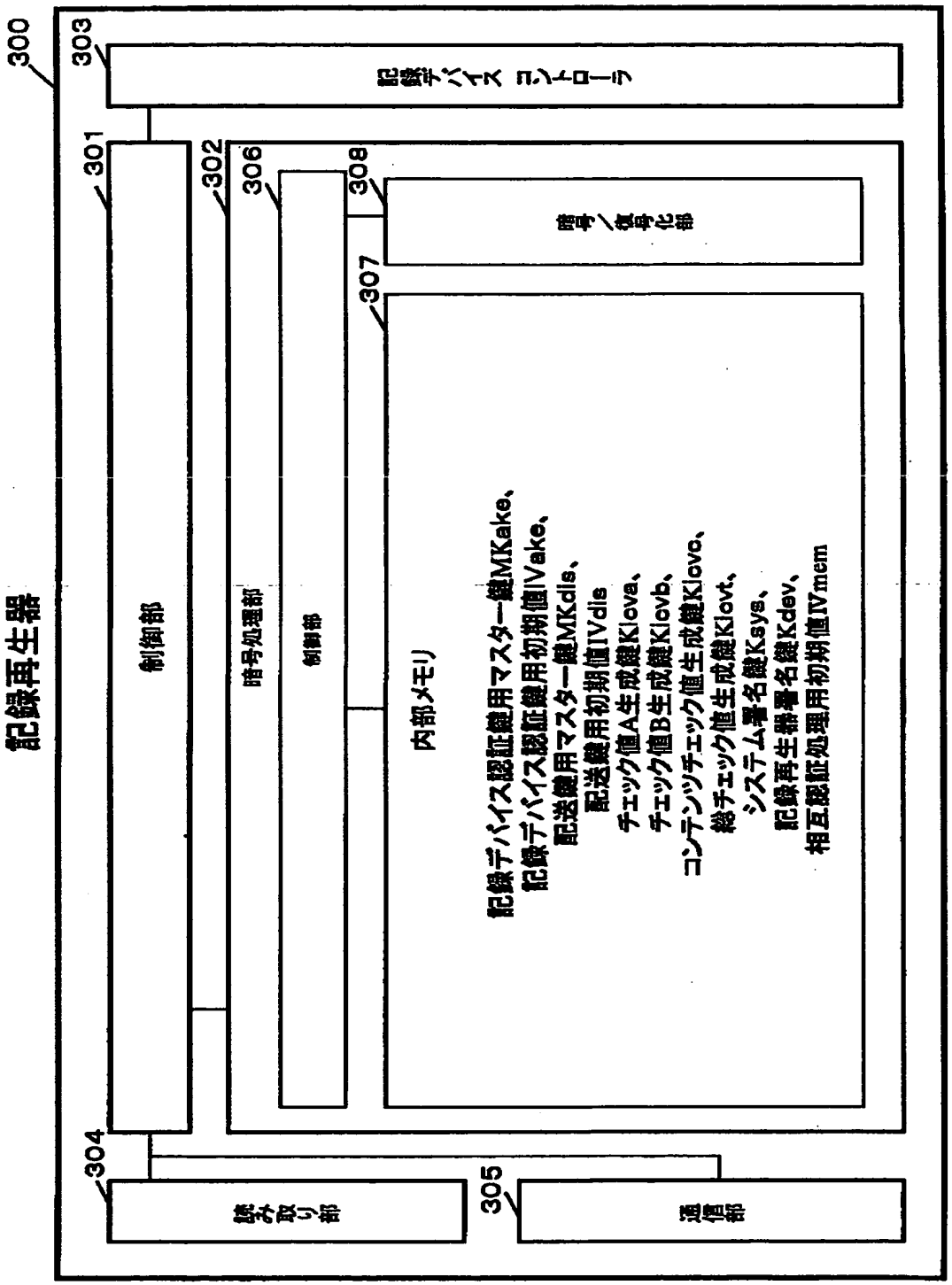
楕円曲線暗号を用いた暗号化（Menezes-Vanstone）

【図１７】

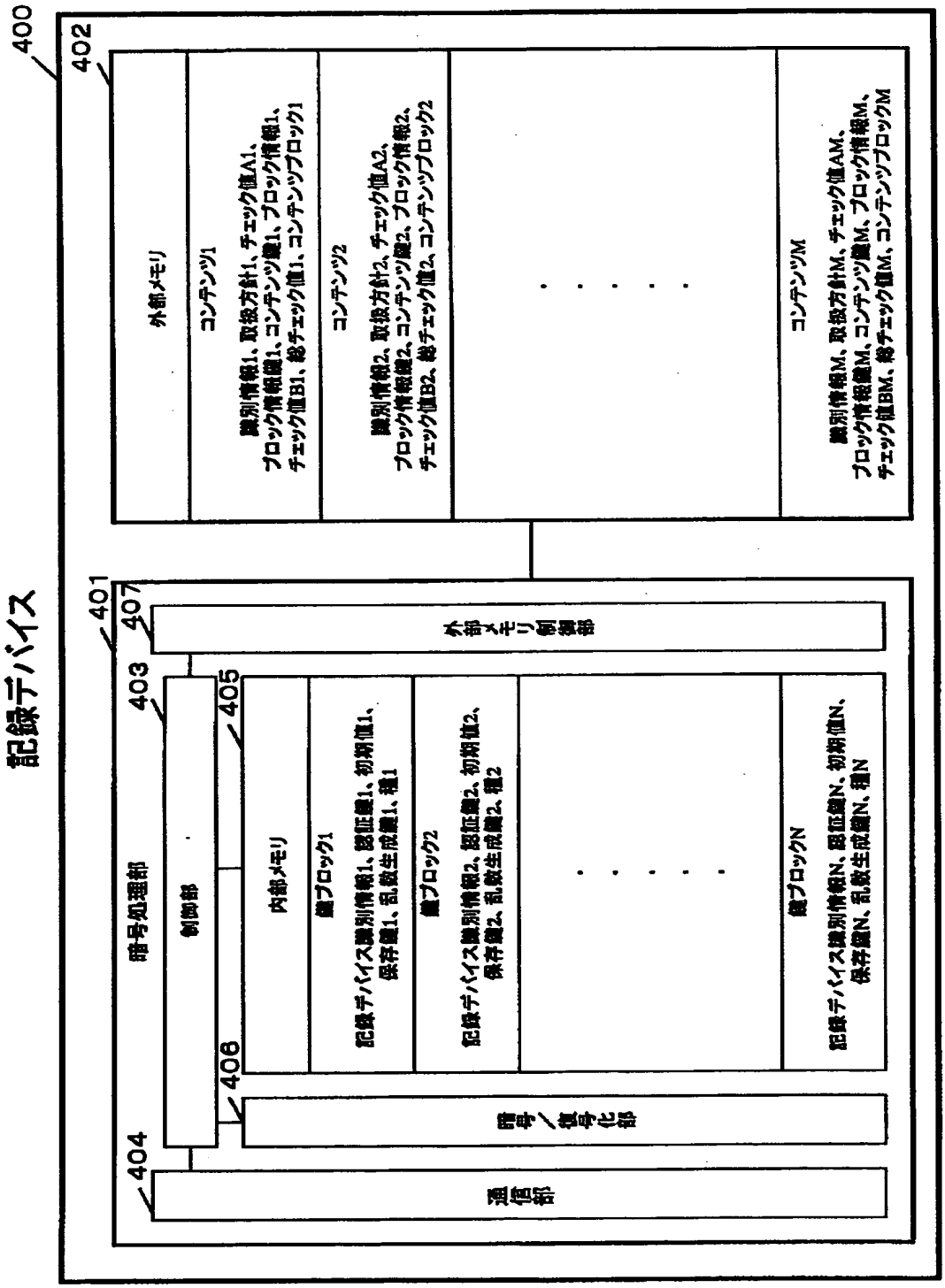


楕円曲線暗号を用いた復号化(Menezes-Vanstone)

【図１８】

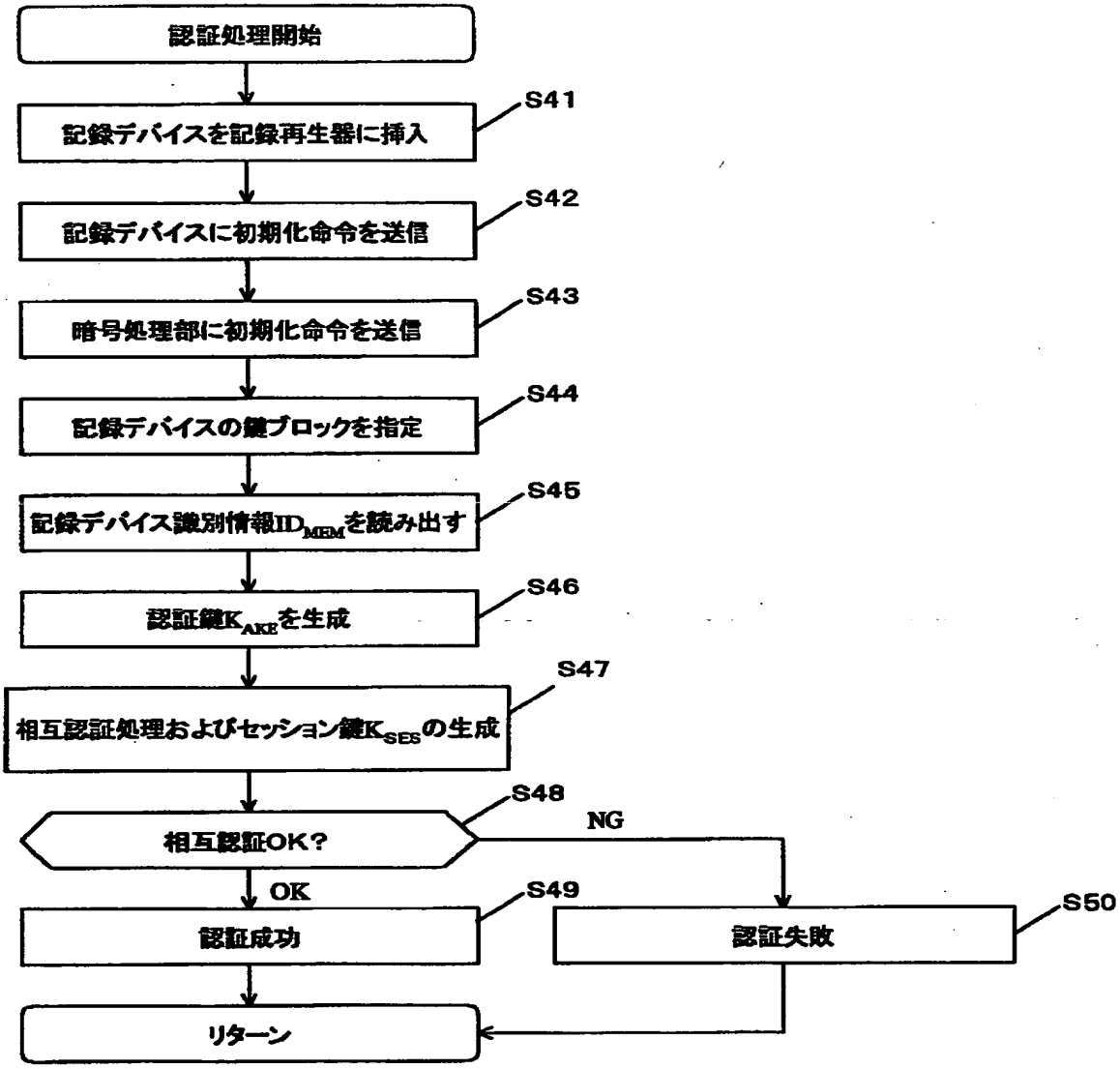

300
303
記録デバイス コントローラ
301
制御部
302
暗号処理部
306
制御部
308
暗号／復号化部
307
内部メモリ
記録デバイス認証鍵用マスター鍵MKake、
記録デバイス認証鍵用初期値IVake、
配送鍵用マスター鍵MKdis、
配送鍵用初期値IVdis
チェック値A生成鍵Klova、
チェック値B生成鍵Klovb、
コンテンツチェック値生成鍵Klovc、
総チェック値生成鍵Klovt、
システム署名鍵Ksys、
記録再生器署名鍵Kdev、
相互認証処理用初期値IVmem
304
305
記録再生器
記録再生器上のデータ保持状況

【図１９】



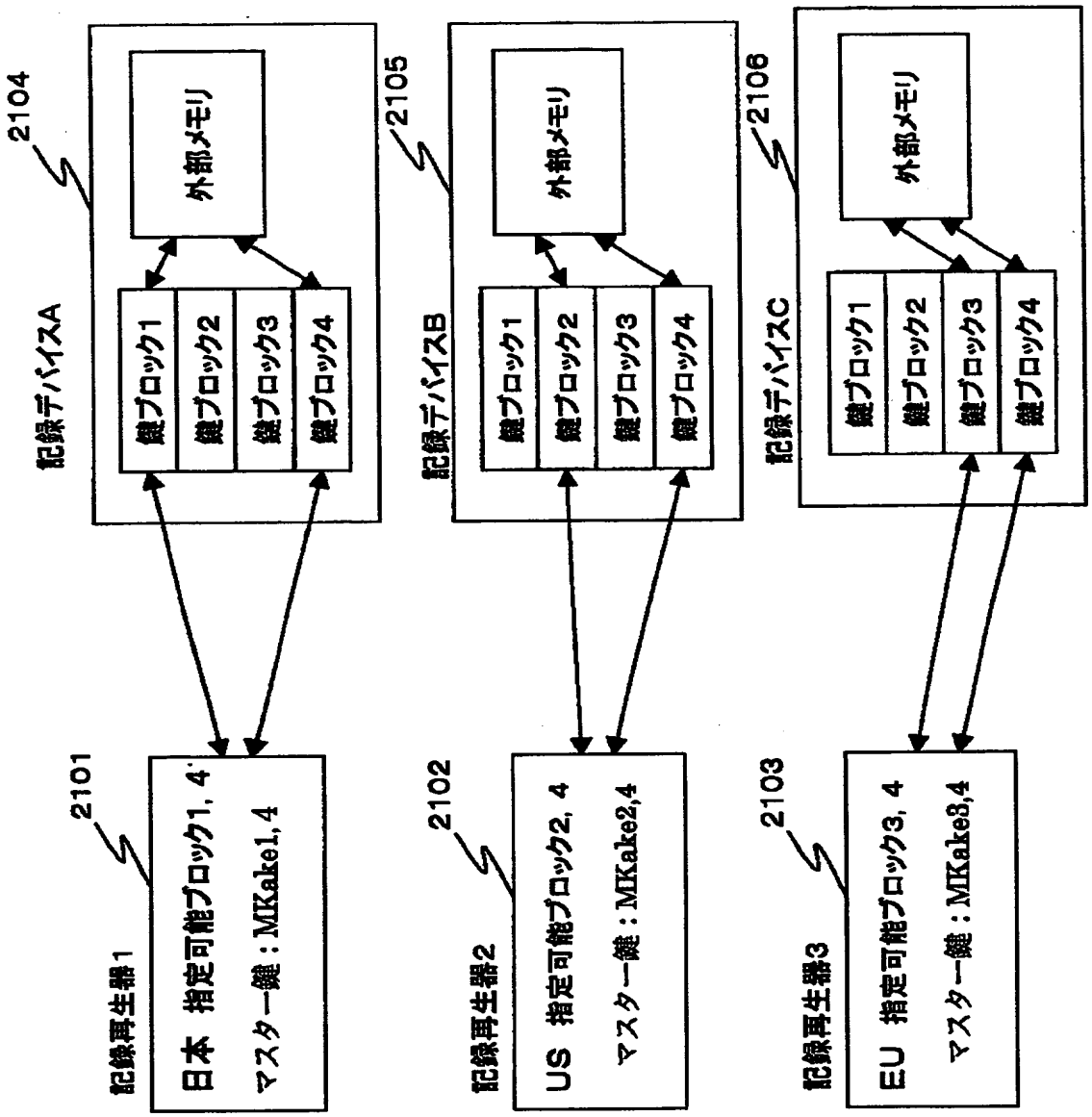
記録デバイス上のデータ保持状況

【図２０】

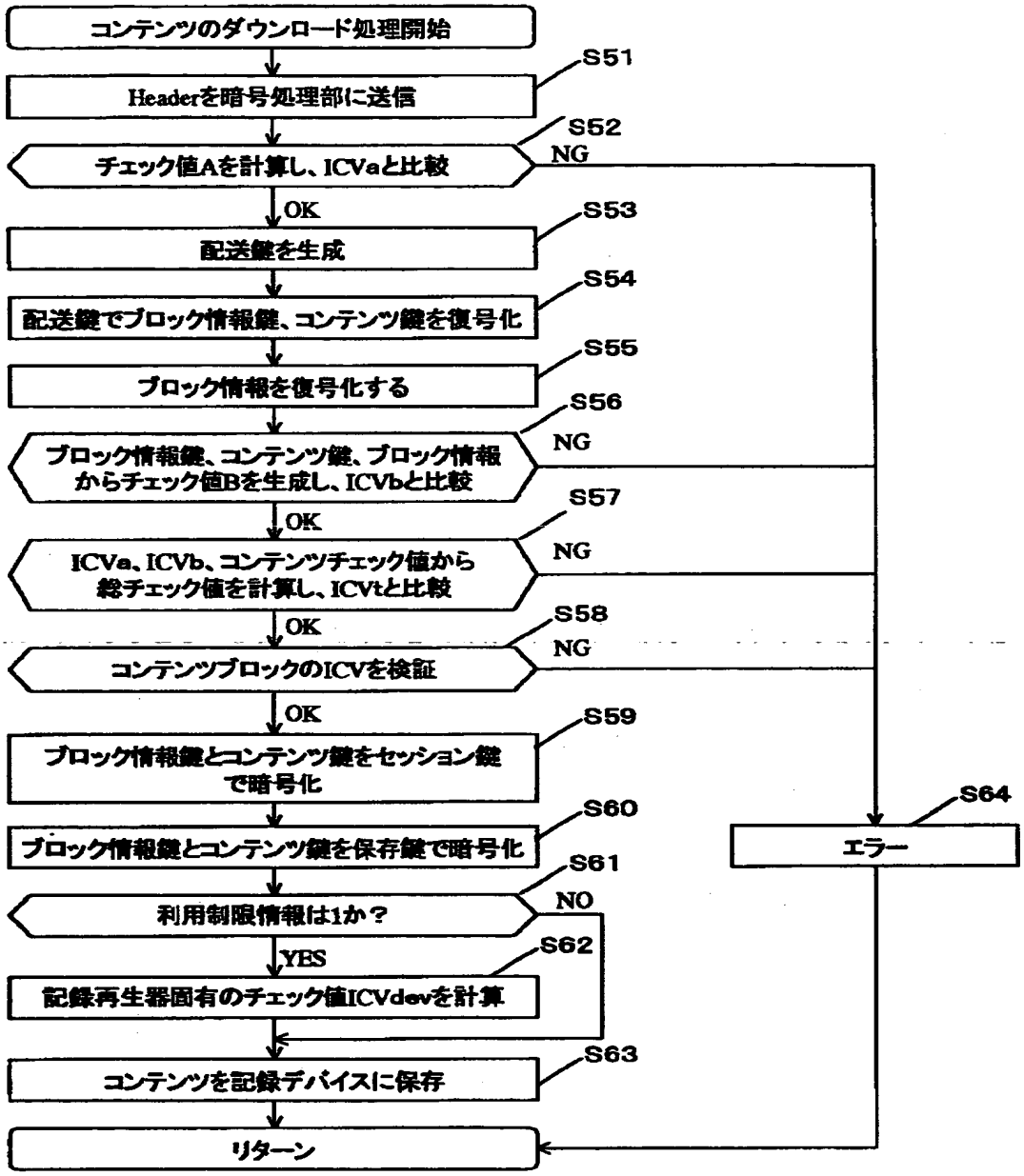


記録再生器と記録デバイスとの相互認証

【図２１】

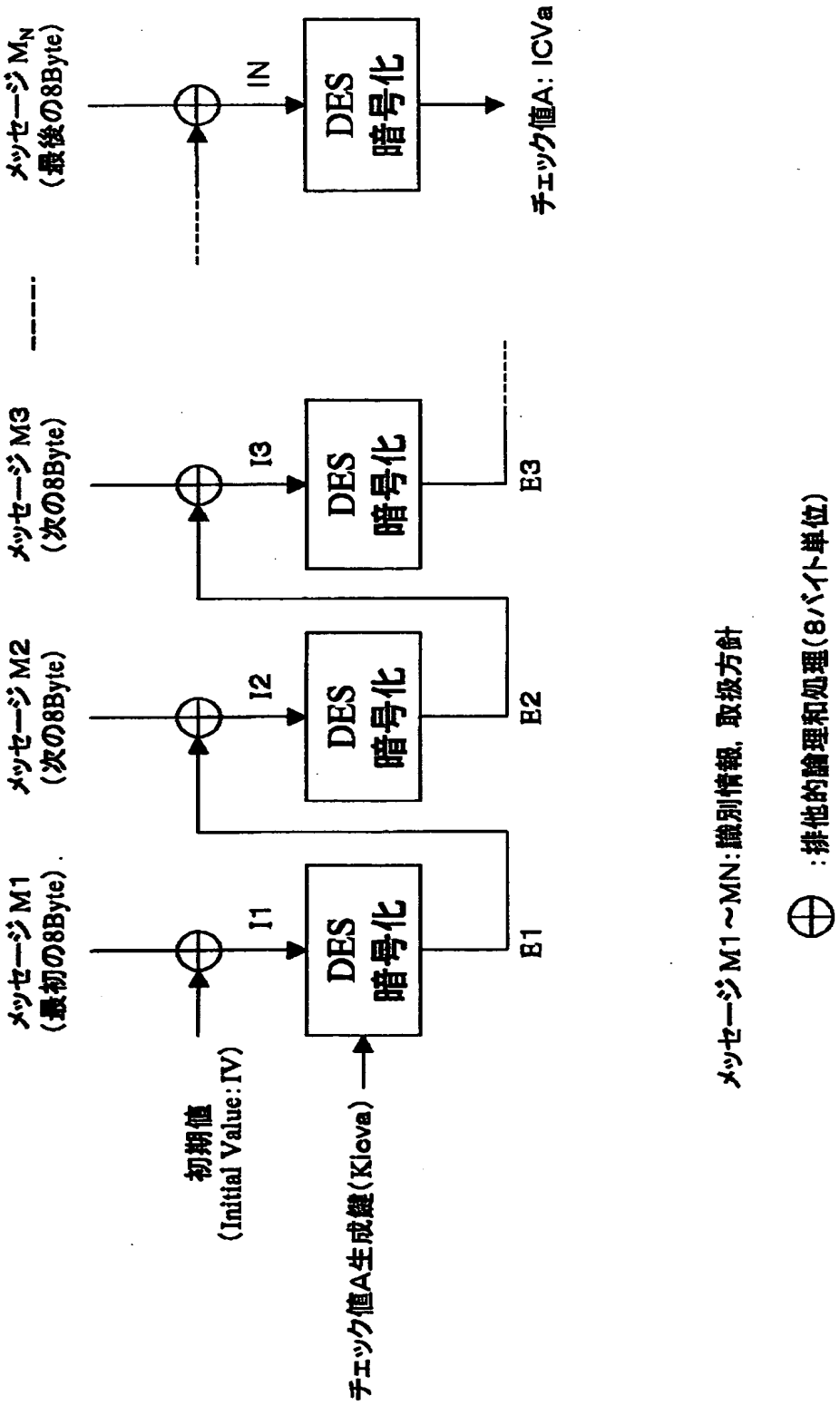

2104
記録デバイスA
外部メモリ
鍵ブロック1
鍵ブロック2
鍵ブロック3
鍵ブロック4
2105
記録デバイスB
外部メモリ
鍵ブロック1
鍵ブロック2
鍵ブロック3
鍵ブロック4
2106
記録デバイスC
外部メモリ
鍵ブロック1
鍵ブロック2
鍵ブロック3
鍵ブロック4
2101
記録再生器1
日本 指定可能ブロック1, 4
マスター鍵：MKake1,4
2102
記録再生器2
US 指定可能ブロック2, 4
マスター鍵：MKake2,4
2103
記録再生器3
EU 指定可能ブロック3, 4
マスター鍵：MKake3,4

【図２２】

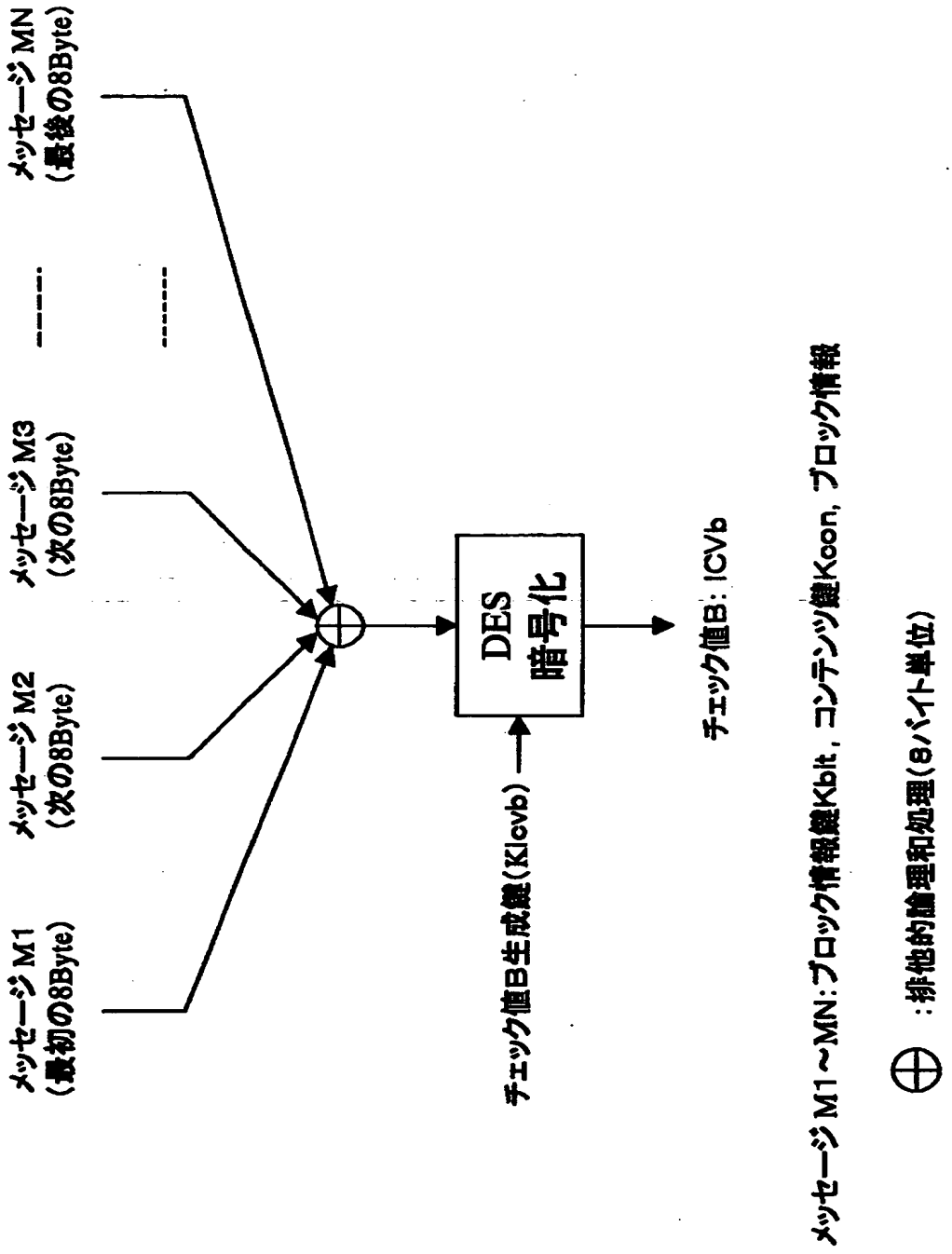


コンテンツのダウンロード処理

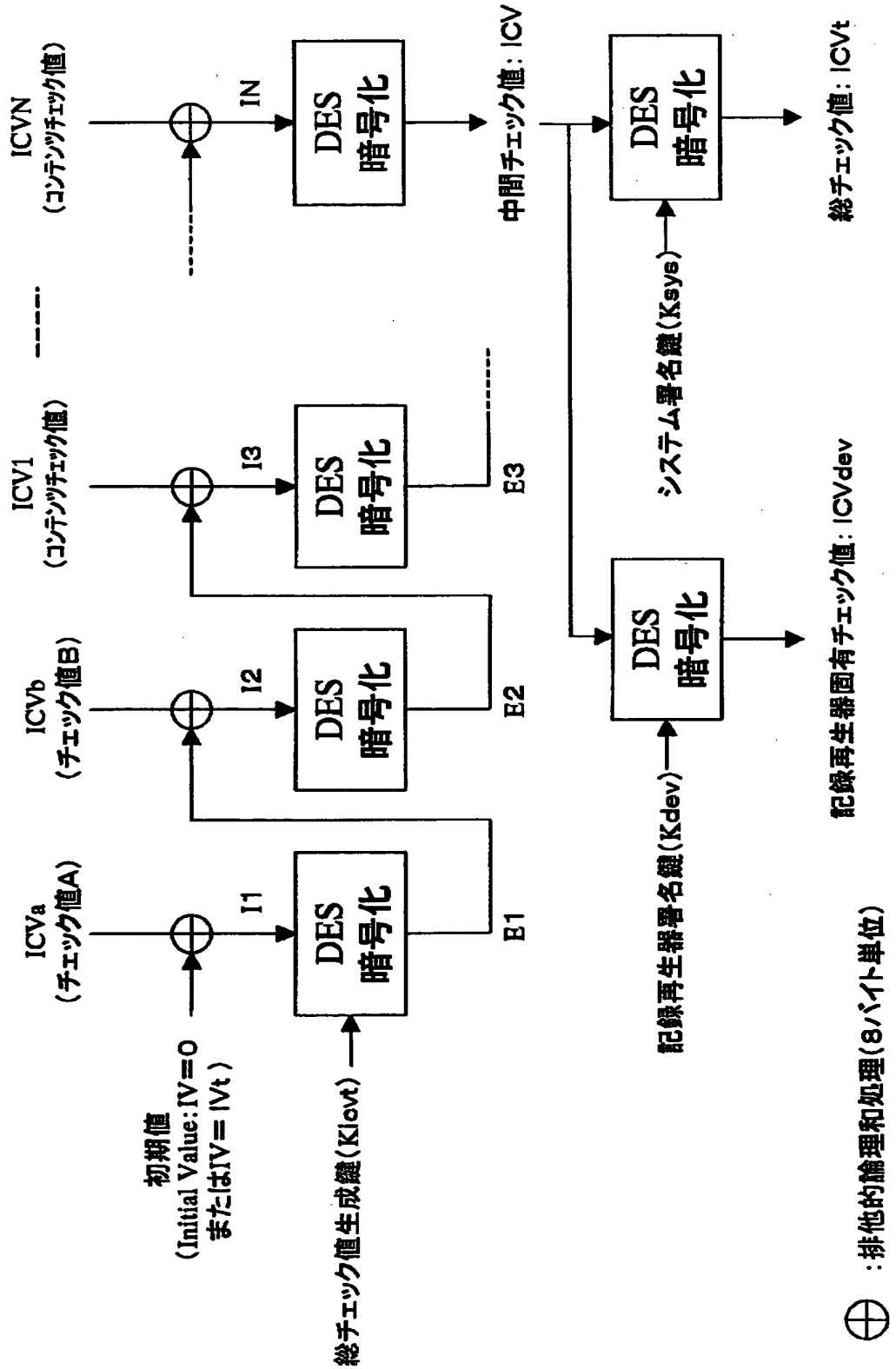
【図２３】


メッセージ M1
(最初の8Byte)
メッセージ M2
(次の8Byte)
メッセージ M3
(次の8Byte)
メッセージ MN
(最後の8Byte)
I1
I2
I3
IN
DES
暗号化
E1
E2
E3
チェック値A: ICVa
初期値
(Initial Value: IV)
チェック値A生成鍵(Klova)
メッセージ M1～MN: 識別情報, 取扱方針
⊕ : 排他的論理和処理(8バイト単位)

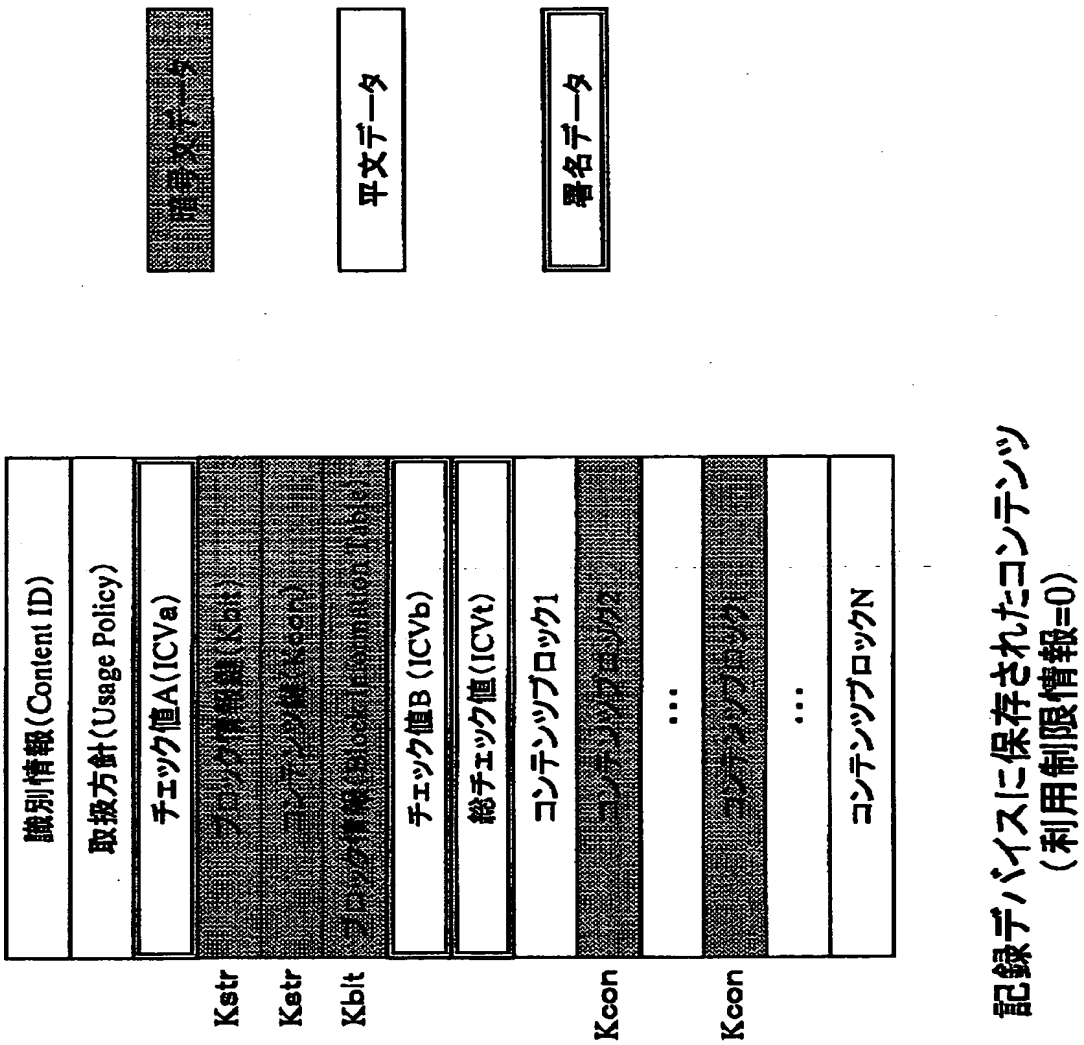
【図２４】


メッセージ MN
(最後の8Byte)
メッセージ M3
(次の8Byte)
メッセージ M2
(次の8Byte)
メッセージ M1
(最初の8Byte)
DES
暗号化
チェック値B生成鍵(Klcvb)
チェック値B: ICVb
メッセージM1～MN:ブロック情報鍵Kblt, コンテンツ鍵Kcon, ブロック情報
⊕ :排他的論理和処理(8バイト単位)

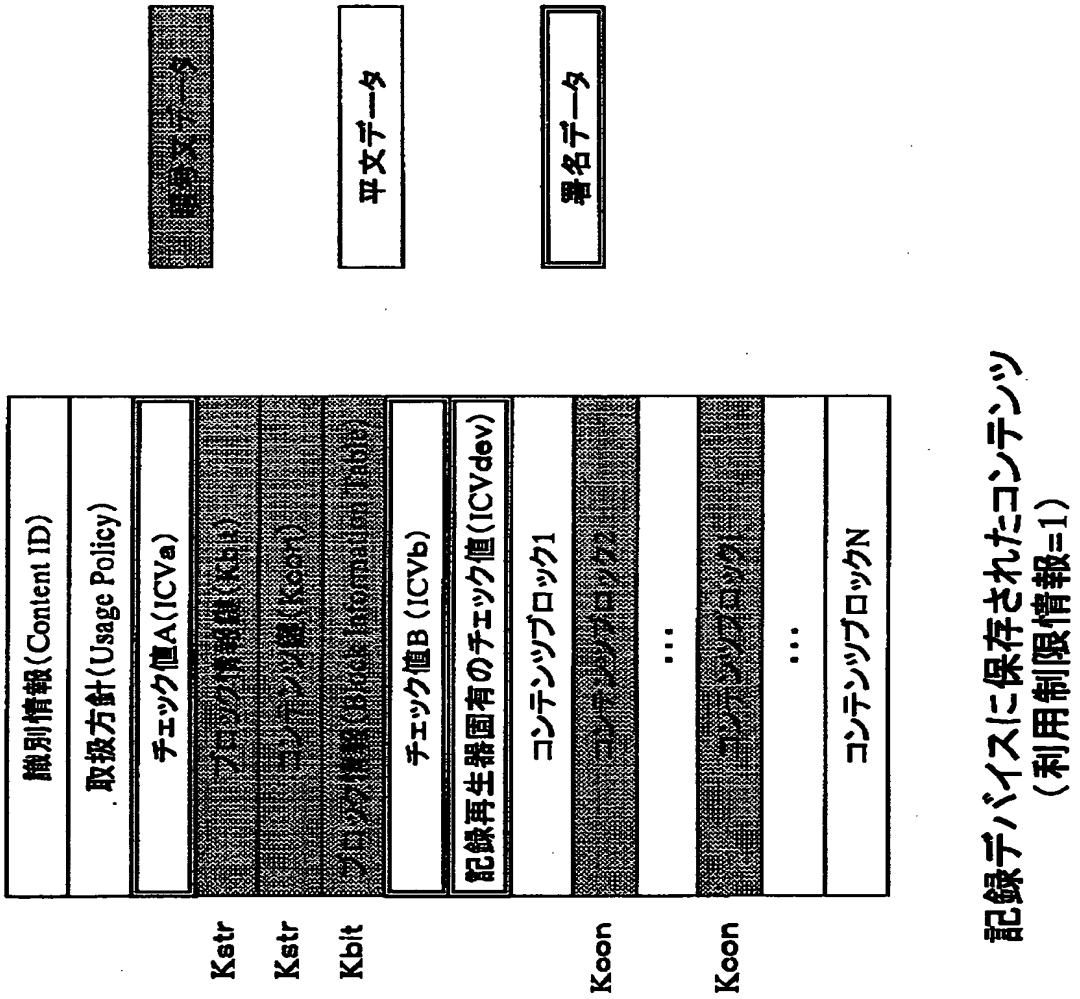
【図２５】


ICVa
(チェック値A)
ICVb
(チェック値B)
ICV1
(コンテンツチェック値)
ICVN
(コンテンツチェック値)
初期値
(Initial Value: IV=0
またはIV= IVt)
I1
I2
I3
IN
DES
暗号化
E1
E2
E3
中間チェック値: ICV
総チェック値生成鍵(Kiovt)
記録再生器署名鍵(Kdev)
システム署名鍵(Ksys)
総チェック値: ICVt
記録再生器固有チェック値: ICVdev
⊕ :排他的論理和処理(8バイト単位)

【図２６】

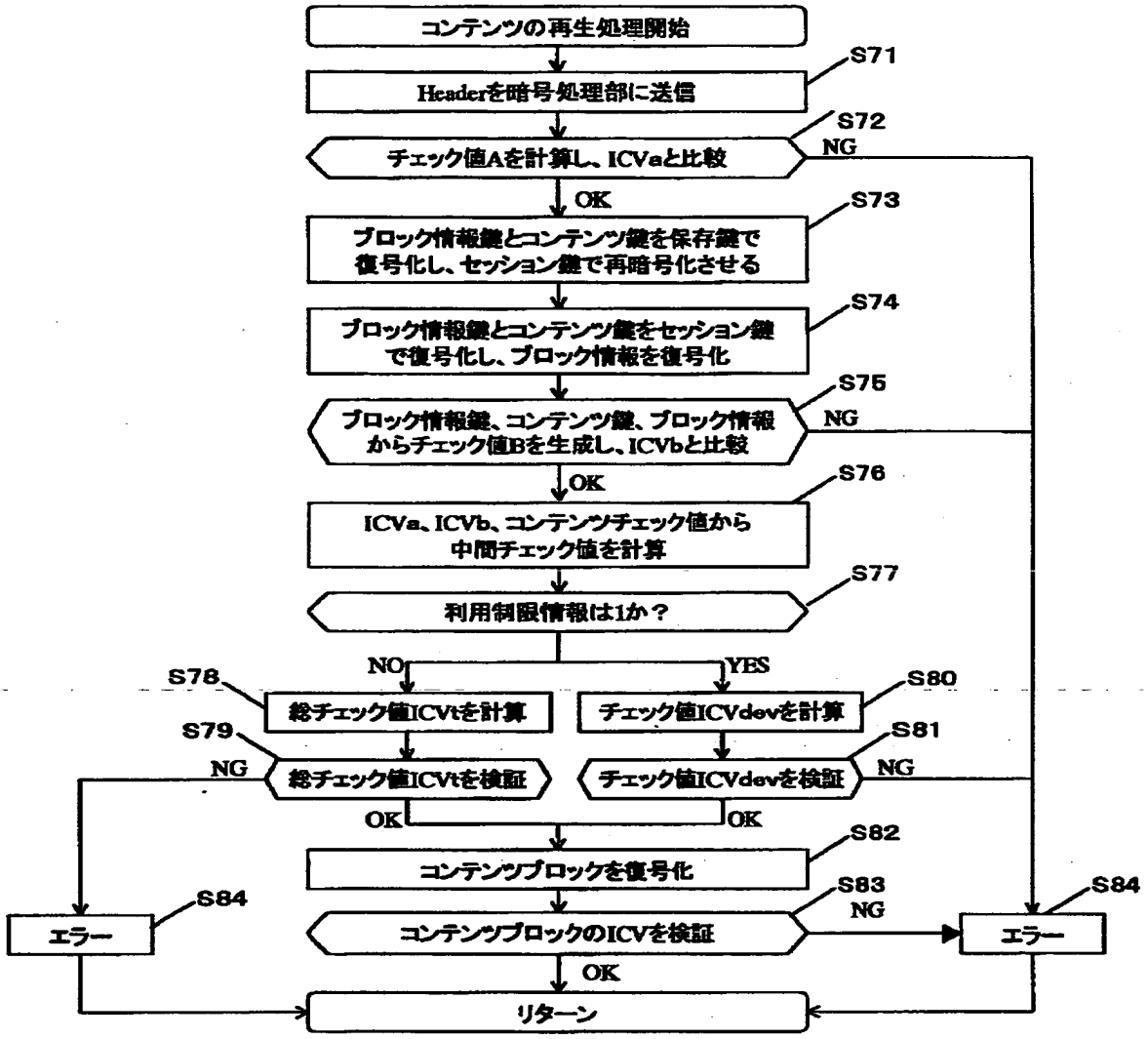

暗号文データ
平文データ
署名データ
識別情報(Content ID)
取扱方針(Usage Policy)
チェック値A(ICVa)
チェック値B (ICVb)
総チェック値(ICVt)
コンテンツブロック1
コンテンツブロックN
Kstr
Kstr
Kblt
Kcon
Kcon
記録デバイスに保存されたコンテンツ
(利用制限情報=0)

【図２７】



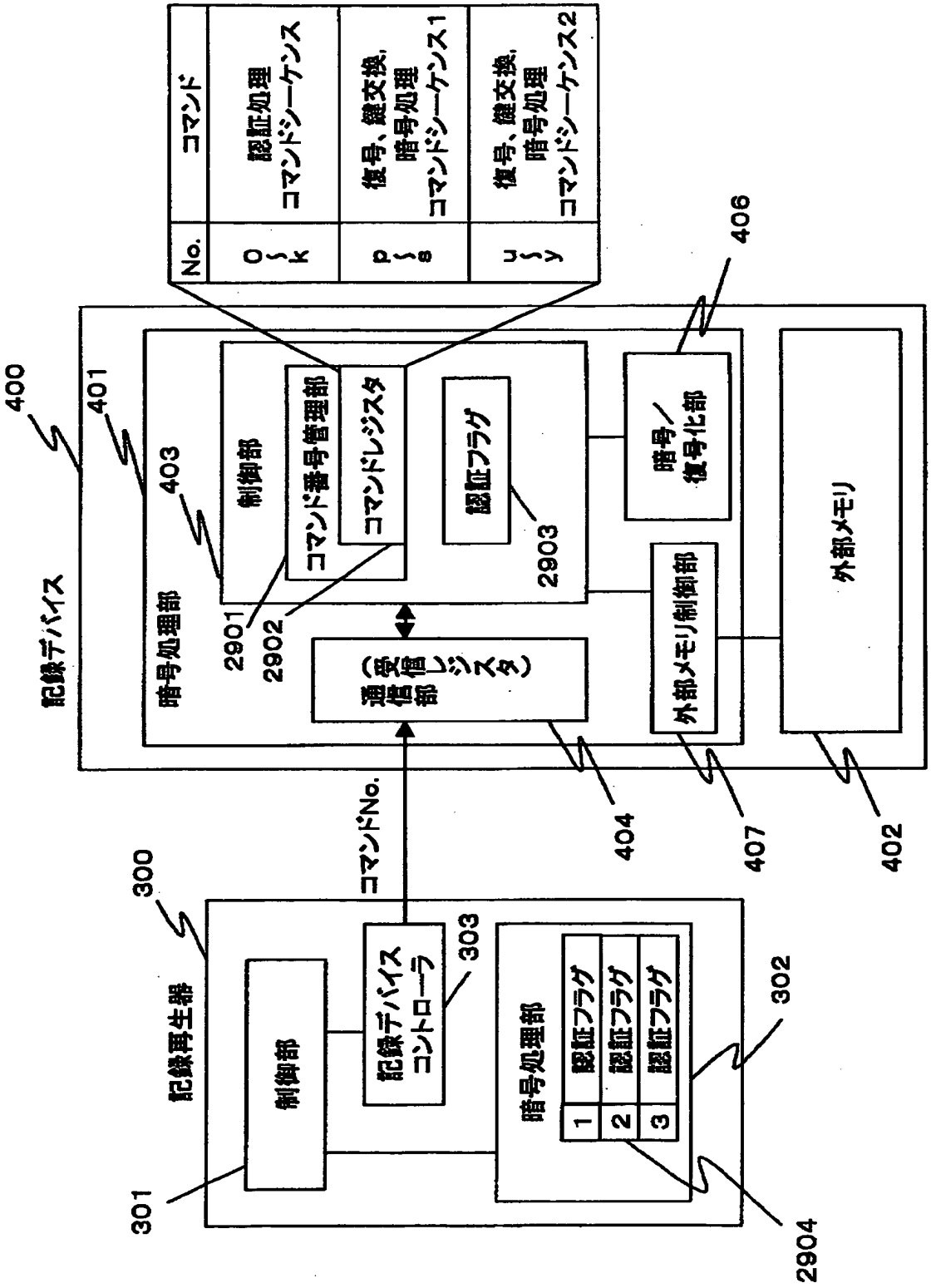
記録デバイスに保存されたコンテンツ
（利用制限情報=1）

【図２８】

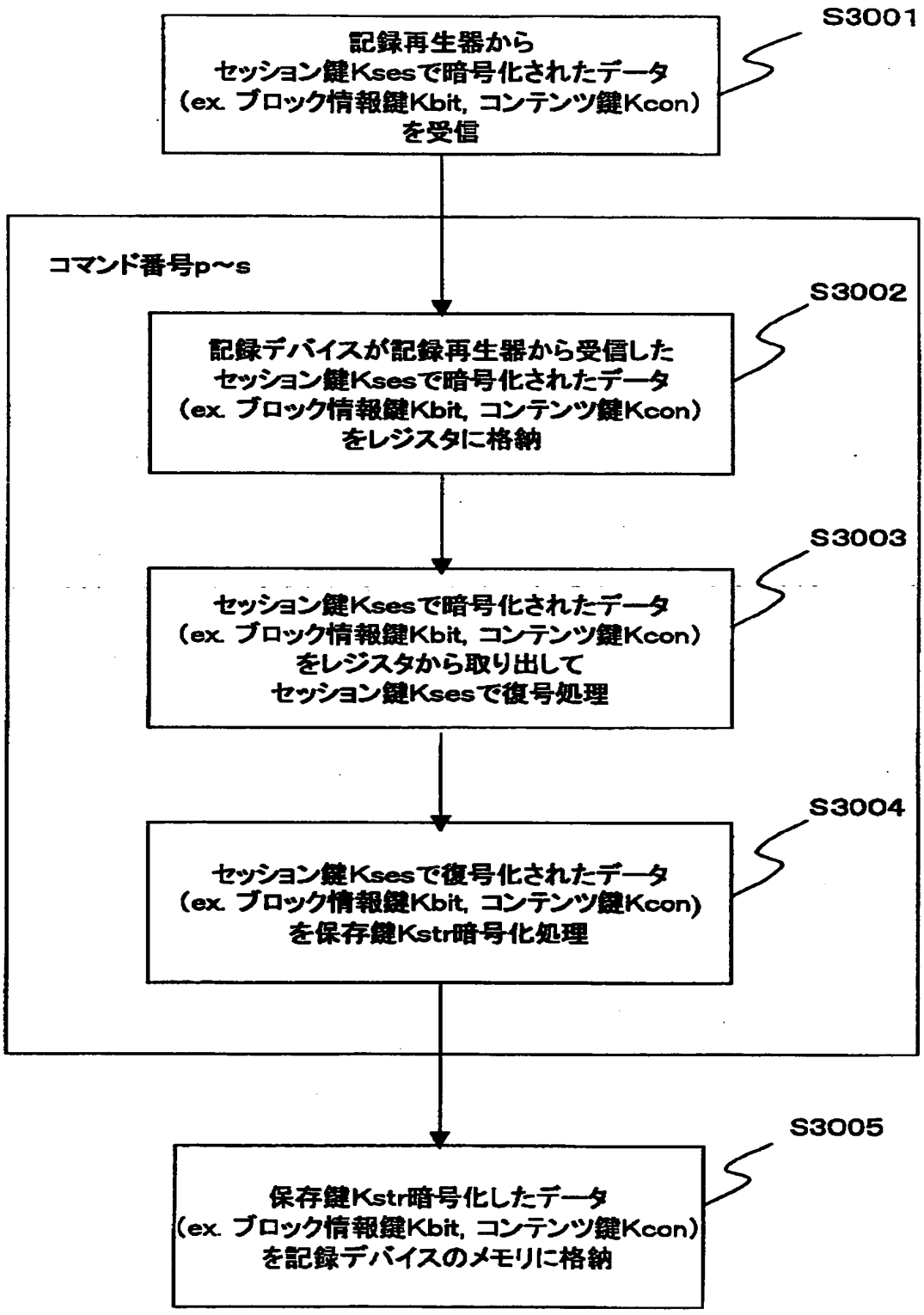


コンテンツの再生処理

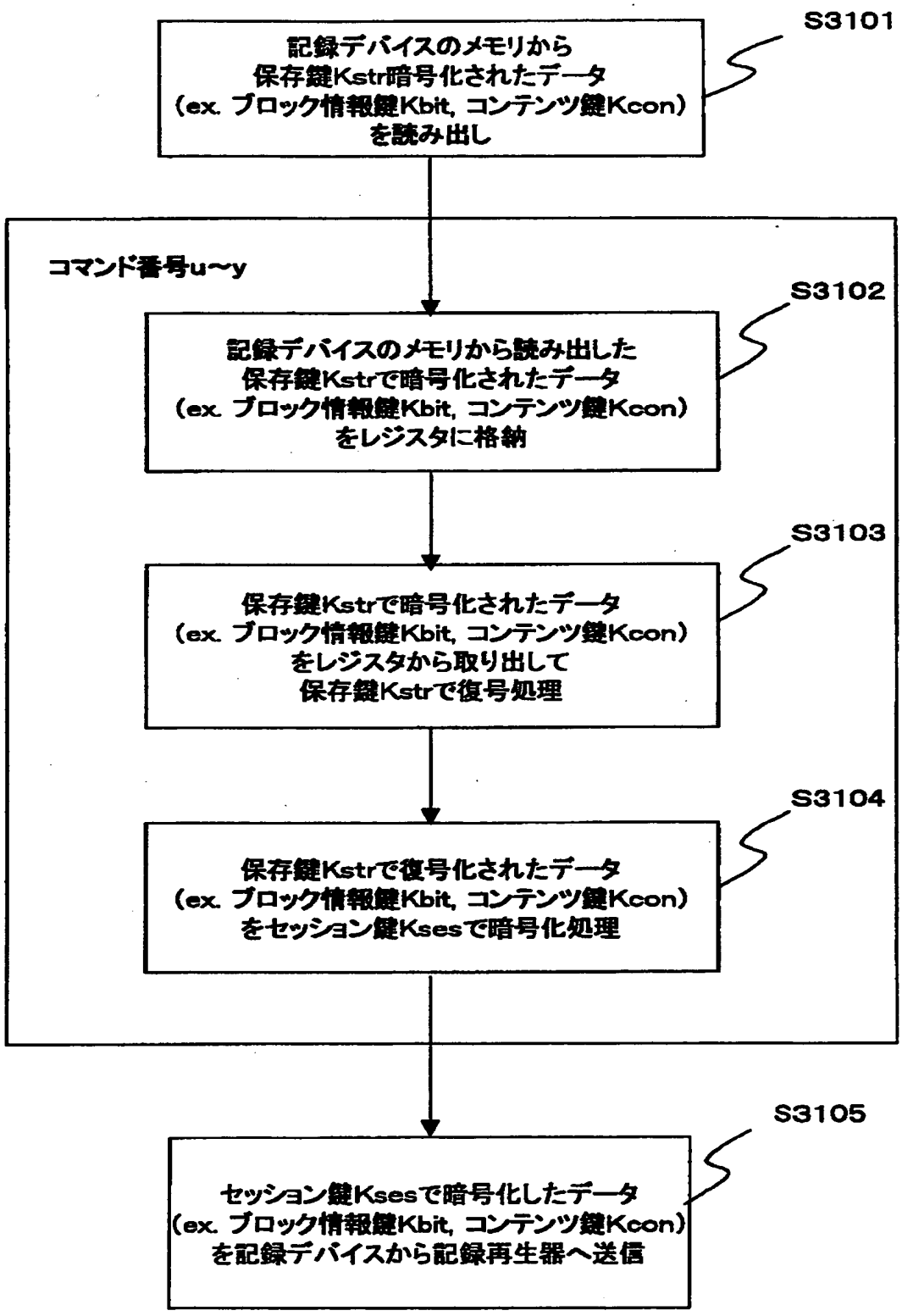
【図２９】


No.
コマンド
0～k
認証処理
コマンドシーケンス
p～s
復号、鍵交換、
暗号処理
コマンドシーケンス1
t～y
復号、鍵交換、
暗号処理
コマンドシーケンス2
400
401
403
406
記録デバイス
暗号処理部
制御部
コマンド番号管理部
コマンドレジスタ
認証フラグ
2903
2901
2902
暗号／
復号化部
外部メモリ制御部
外部メモリ
(受信レジスタ)
送信部
404
407
402
コマンドNo.
300
記録再生器
制御部
記録デバイス
コントローラ
303
暗号処理部
1
2
3
認証フラグ
認証フラグ
認証フラグ
302
301
2904

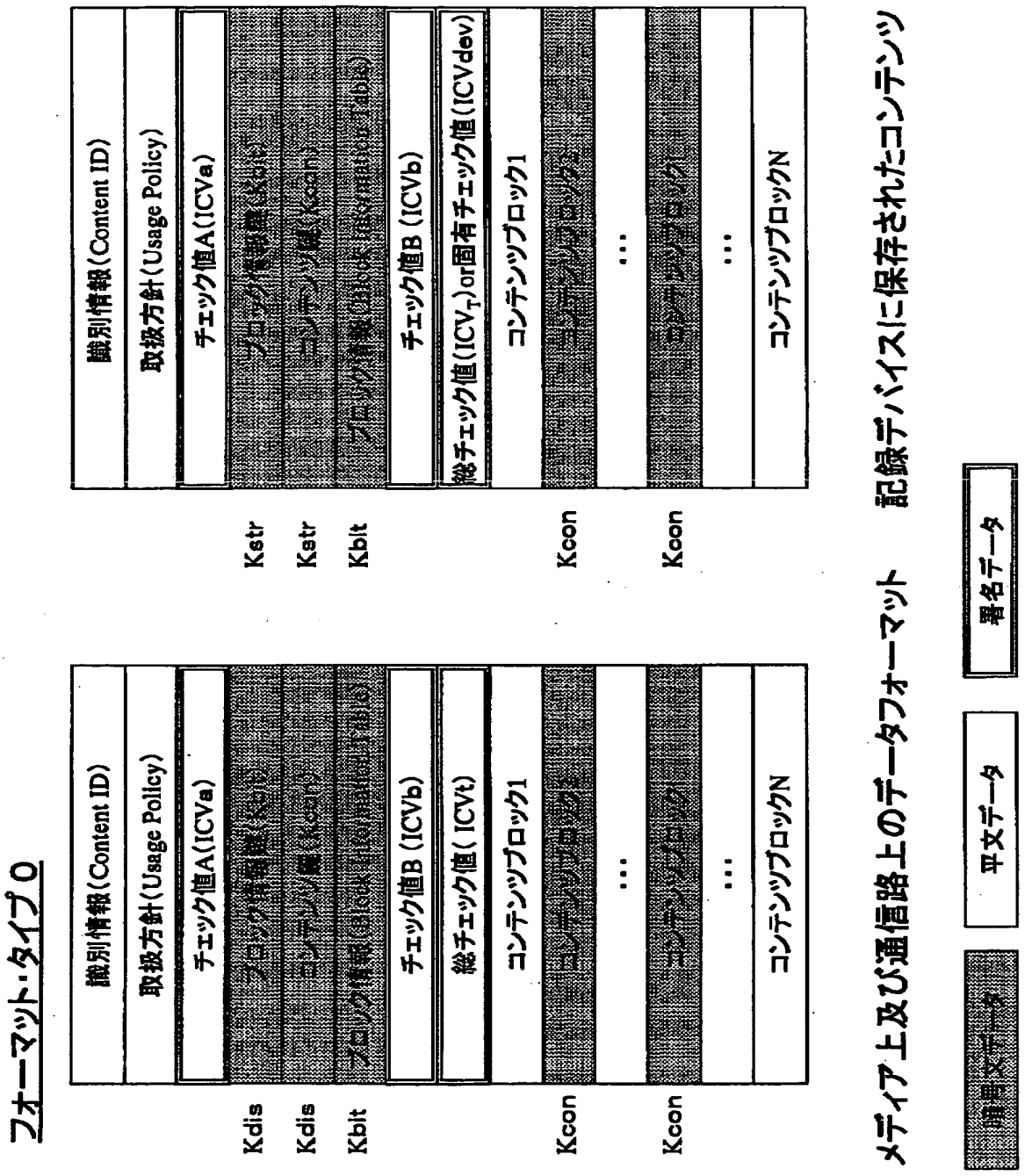
【図３０】


S3001
記録再生器から
セッション鍵Ksesで暗号化されたデータ
(ex. ブロック情報鍵Kbit, コンテンツ鍵Kcon)
を受信
コマンド番号p～s
S3002
記録デバイスが記録再生器から受信した
セッション鍵Ksesで暗号化されたデータ
(ex. ブロック情報鍵Kbit, コンテンツ鍵Kcon)
をレジスタに格納
S3003
セッション鍵Ksesで暗号化されたデータ
(ex. ブロック情報鍵Kbit, コンテンツ鍵Kcon)
をレジスタから取り出して
セッション鍵Ksesで復号処理
S3004
セッション鍵Ksesで復号化されたデータ
(ex. ブロック情報鍵Kbit, コンテンツ鍵Kcon)
を保存鍵Kstr暗号化処理
S3005
保存鍵Kstr暗号化したデータ
(ex. ブロック情報鍵Kbit, コンテンツ鍵Kcon)
を記録デバイスのメモリに格納

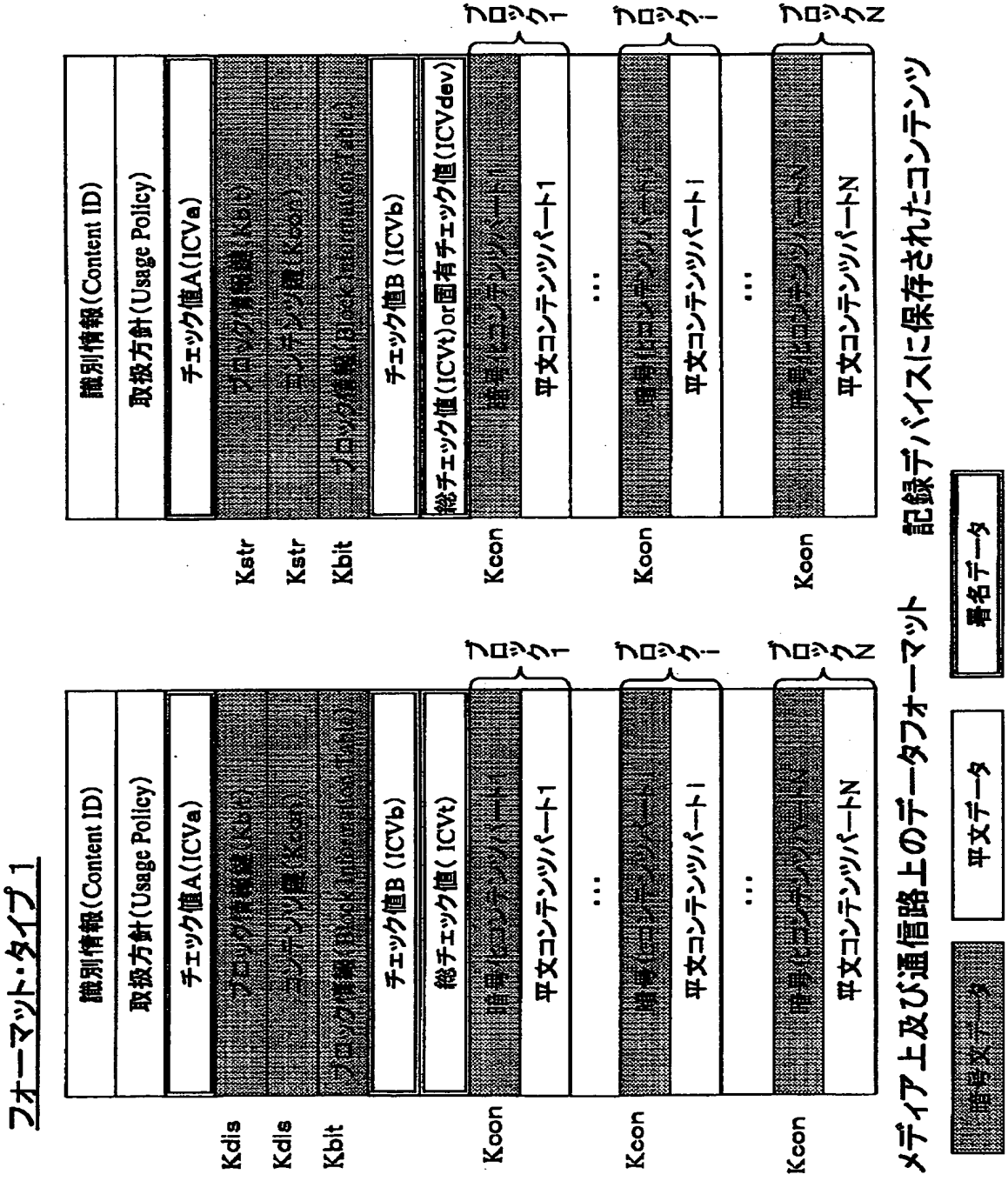
【図３１】


S3101
記録デバイスのメモリから
保存鍵Kstr暗号化されたデータ
(ex. ブロック情報鍵Kbit, コンテンツ鍵Kcon)
を読み出し
コマンド番号u~y
S3102
記録デバイスのメモリから読み出した
保存鍵Kstrで暗号化されたデータ
(ex. ブロック情報鍵Kbit, コンテンツ鍵Kcon)
をレジスタに格納
S3103
保存鍵Kstrで暗号化されたデータ
(ex. ブロック情報鍵Kbit, コンテンツ鍵Kcon)
をレジスタから取り出して
保存鍵Kstrで復号処理
S3104
保存鍵Kstrで復号化されたデータ
(ex. ブロック情報鍵Kbit, コンテンツ鍵Kcon)
をセッション鍵Ksesで暗号化処理
S3105
セッション鍵Ksesで暗号化したデータ
(ex. ブロック情報鍵Kbit, コンテンツ鍵Kcon)
を記録デバイスから記録再生器へ送信

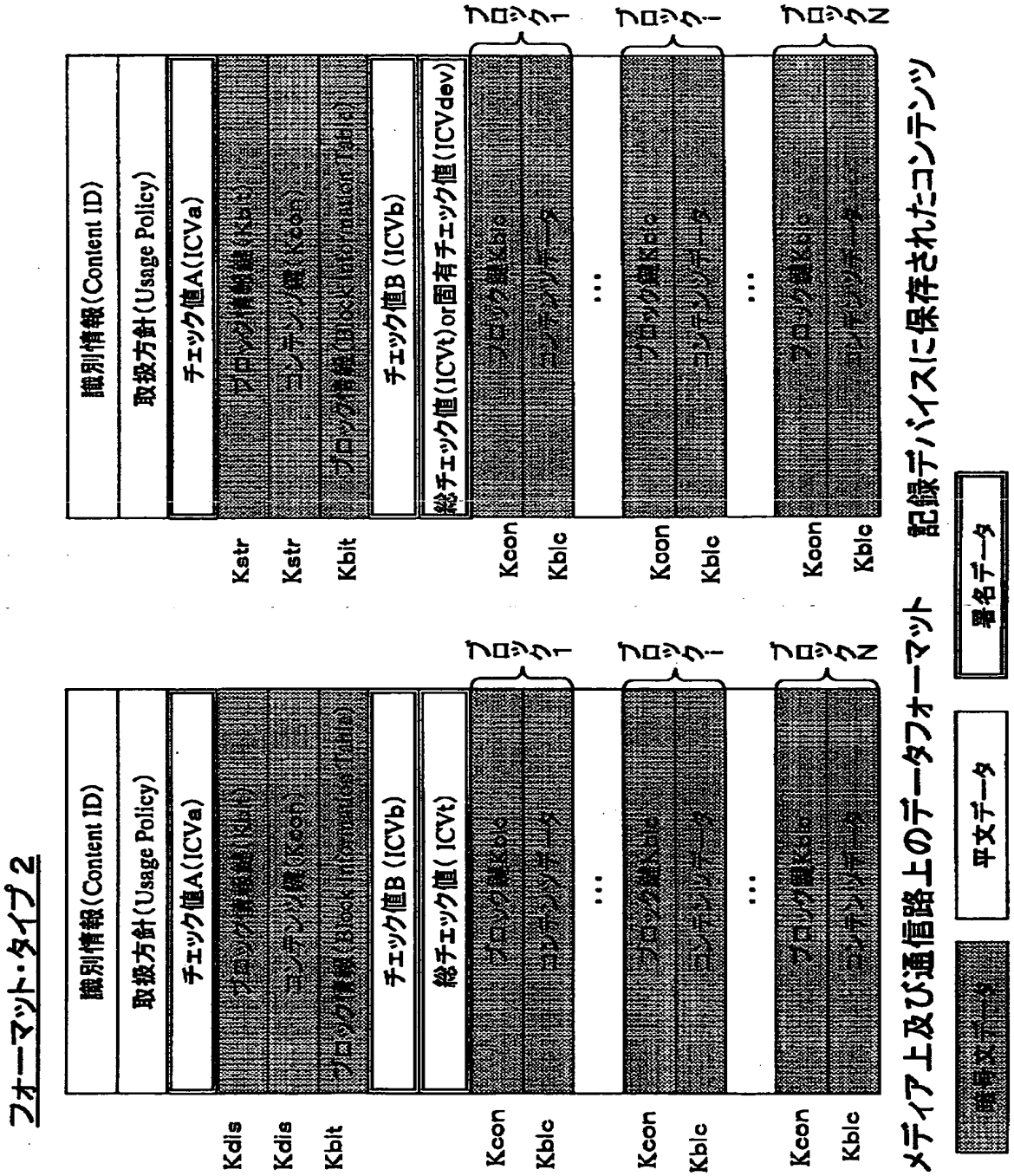
【図３２】


フォーマット・タイプ０
識別情報(Content ID)
取扱方針(Usage Policy)
チェック値A(ICVa)
ブロック情報(Kdis)
コンテンツ鍵(Kcon)
ブロック情報(Kbit)
チェック値B (ICVb)
総チェック値(ICVt)
コンテンツブロック1
コンテンツブロック2
コンテンツブロック3
コンテンツブロックN
Kdis
Kdis
Kbit
Kcon
Kcon
識別情報(Content ID)
取扱方針(Usage Policy)
チェック値A(ICVa)
ブロック情報(Kstr)
コンテンツ鍵(Kcon)
ブロック情報(Kbit)
チェック値B (ICVb)
総チェック値(ICVT)or固有チェック値(ICVdev)
コンテンツブロック1
コンテンツブロック2
コンテンツブロック3
コンテンツブロックN
Kstr
Kstr
Kbit
Kcon
Kcon
メディア上及び通信路上のデータフォーマット
記録デバイスに保存されたコンテンツ
暗号文データ
平文データ
署名データ

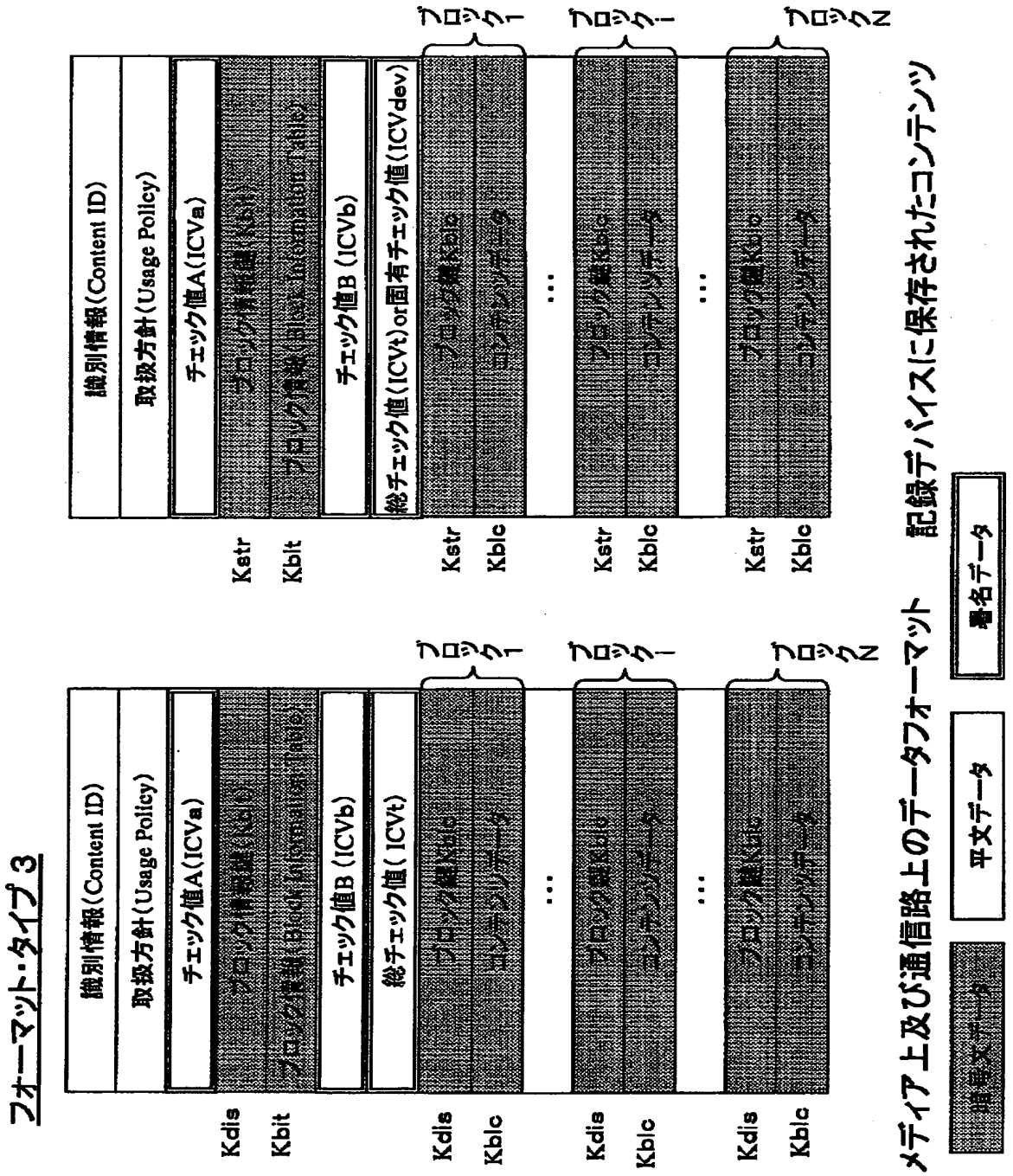
【図３３】


フォーマット・タイプ１
識別情報(Content ID)
取扱方針(Usage Policy)
チェック値A(ICVa)
ブロック情報(Kdis)
コンテンツ鍵(Kcon)
ブロック情報(Block Length)
チェック値B (ICVb)
総チェック値(ICVt)
暗号化コンテンツパート1
平文コンテンツパート1
暗号化コンテンツパートN
平文コンテンツパートN
Kdis
Kbit
Kcon
ブロック1
ブロックN
メディア上及び通信路上のデータフォーマット
記録デバイスに保存されたコンテンツ
暗号文データ
平文データ
署名データ

【図３４】

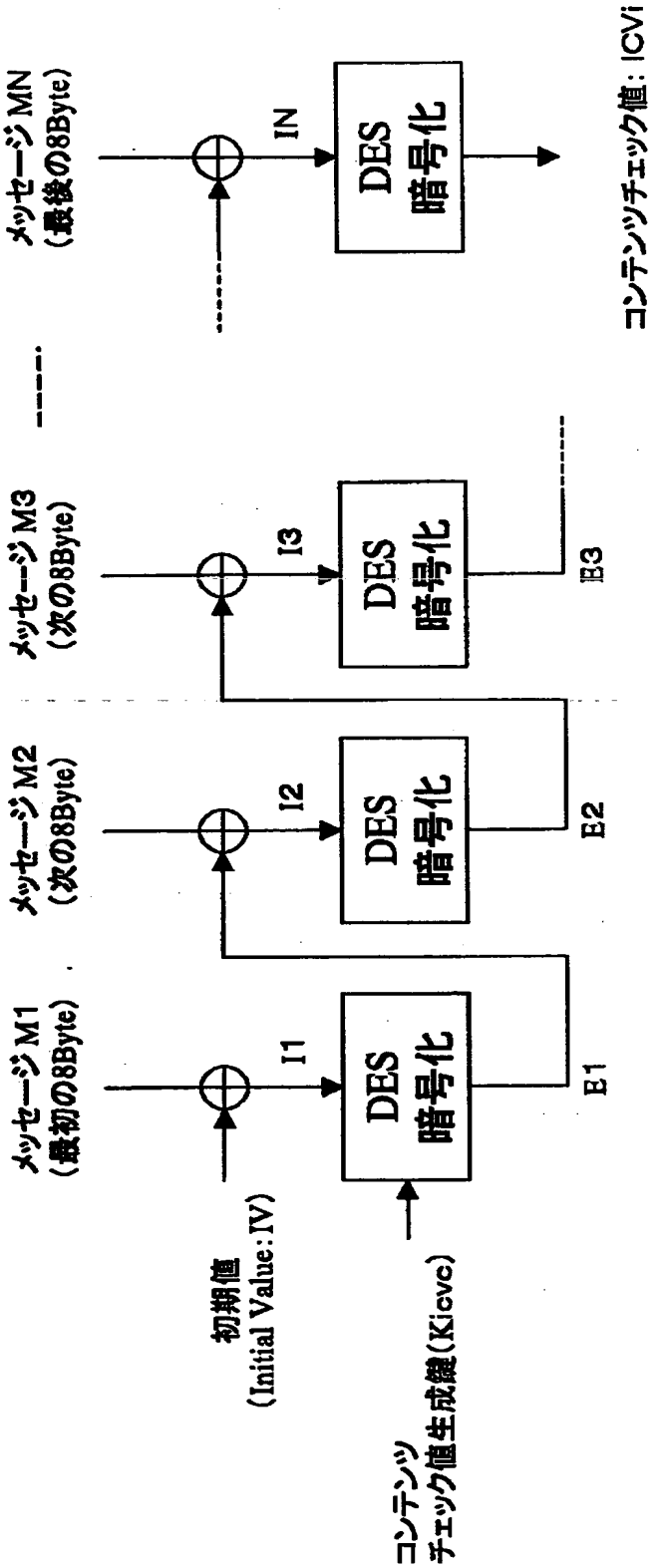

フォーマット・タイプ２
識別情報(Content ID)
取扱方針(Usage Policy)
チェック値A(ICVa)
ブロック情報(Block Information Table)
チェック値B (ICVb)
総チェック値(ICVt)
ブロック1
ブロックN
Kdis
Kdis
Kbit
Kcon
Kblc
メディア上及び通信路上のデータフォーマット
記録デバイスに保存されたコンテンツ
暗号文データ
平文データ
署名データ

【図３５】

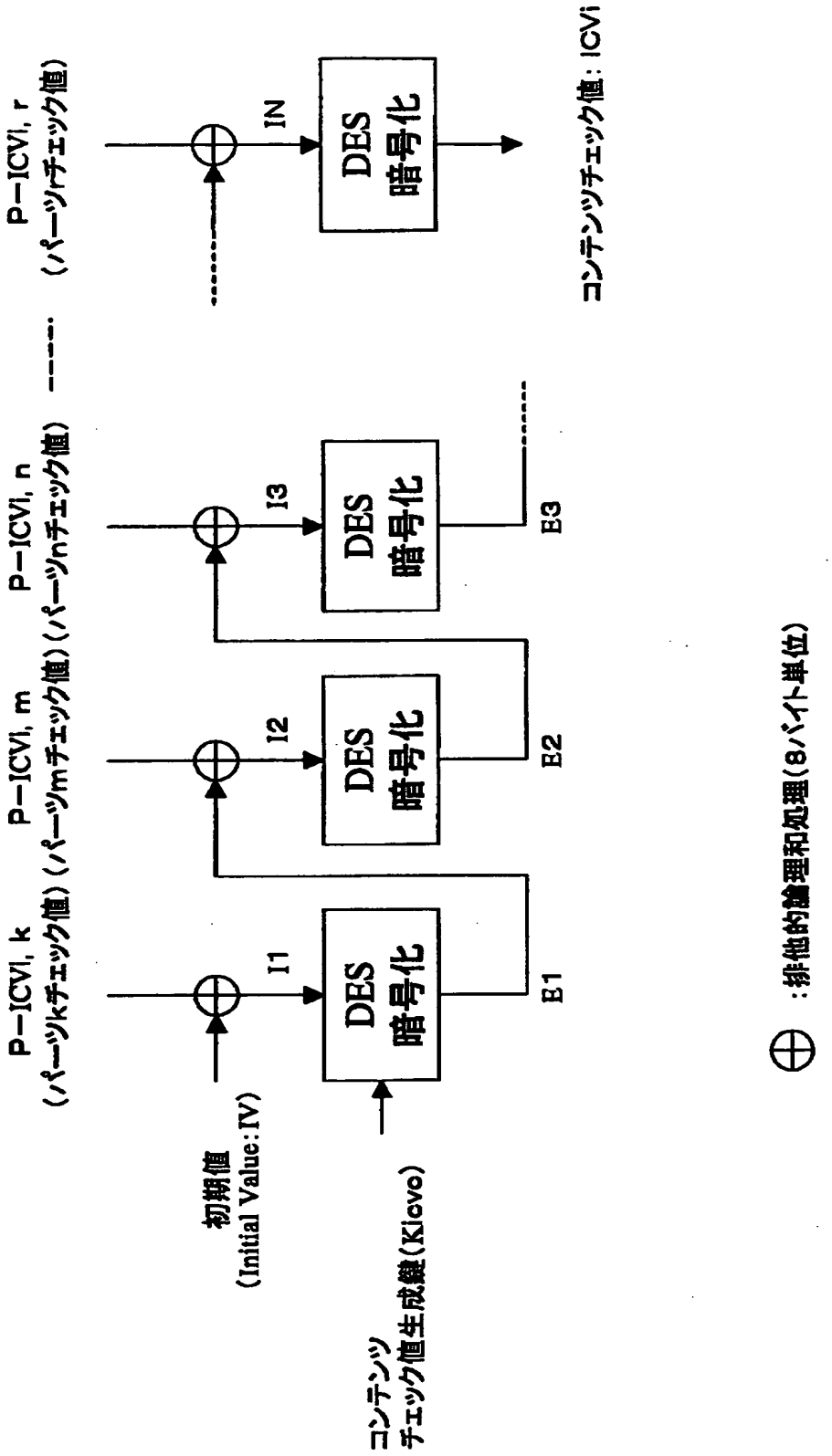


出証特２０００－３１０２４６７

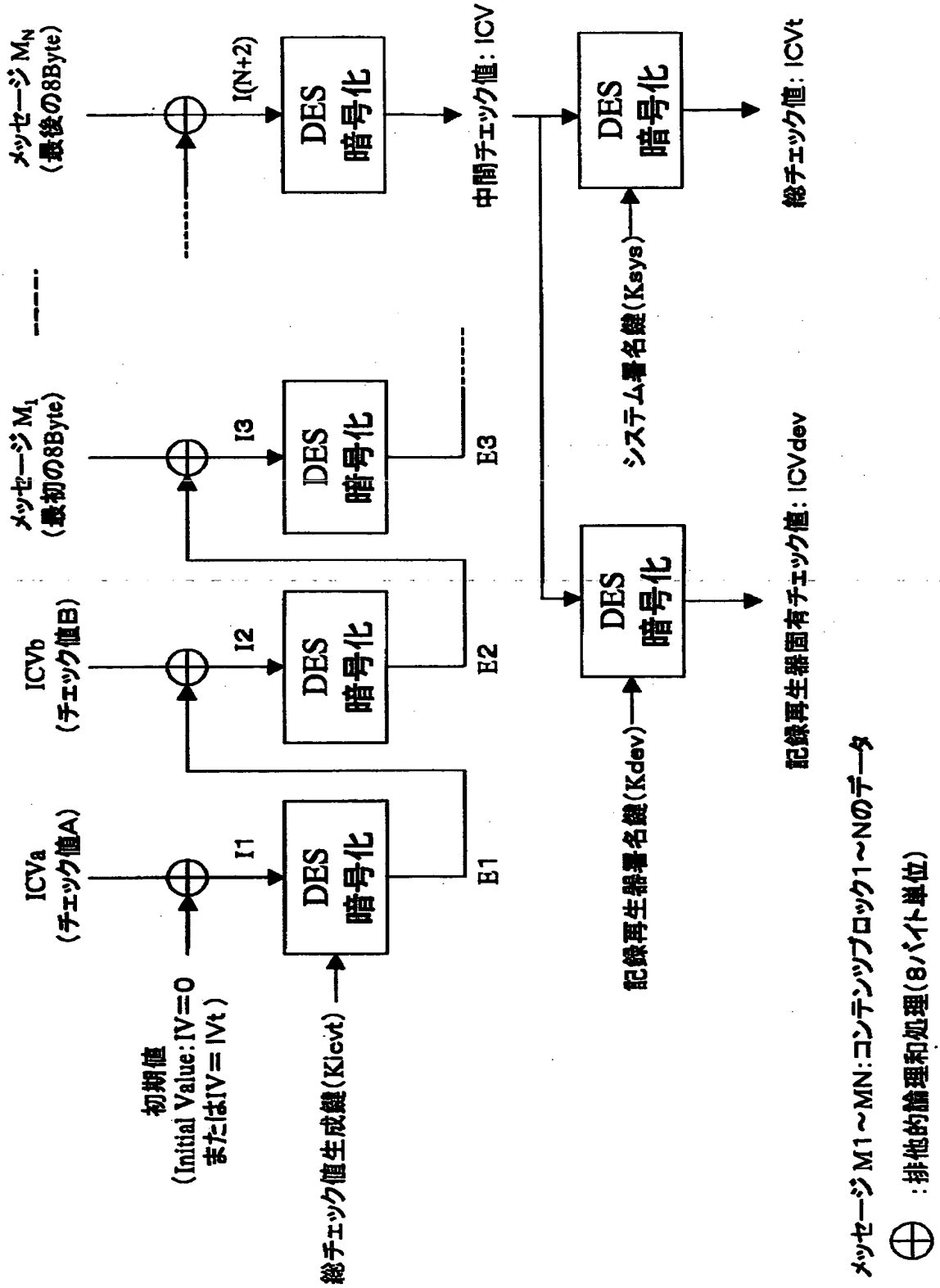
【図３６】


メッセージ M1
(最初の8Byte)
メッセージ M2
(次の8Byte)
メッセージ M3
(次の8Byte)
メッセージ MN
(最後の8Byte)
I1
I2
I3
IN
DES
暗号化
E1
E2
E3
初期値
(Initial Value:IV)
コンテンツ
チェック値生成鍵(Kicvc)
コンテンツチェック値: ICVi
メッセージ M1～MN:コンテンツのコンテンツデータ
⊕ :排他的論理和処理(8バイト単位)

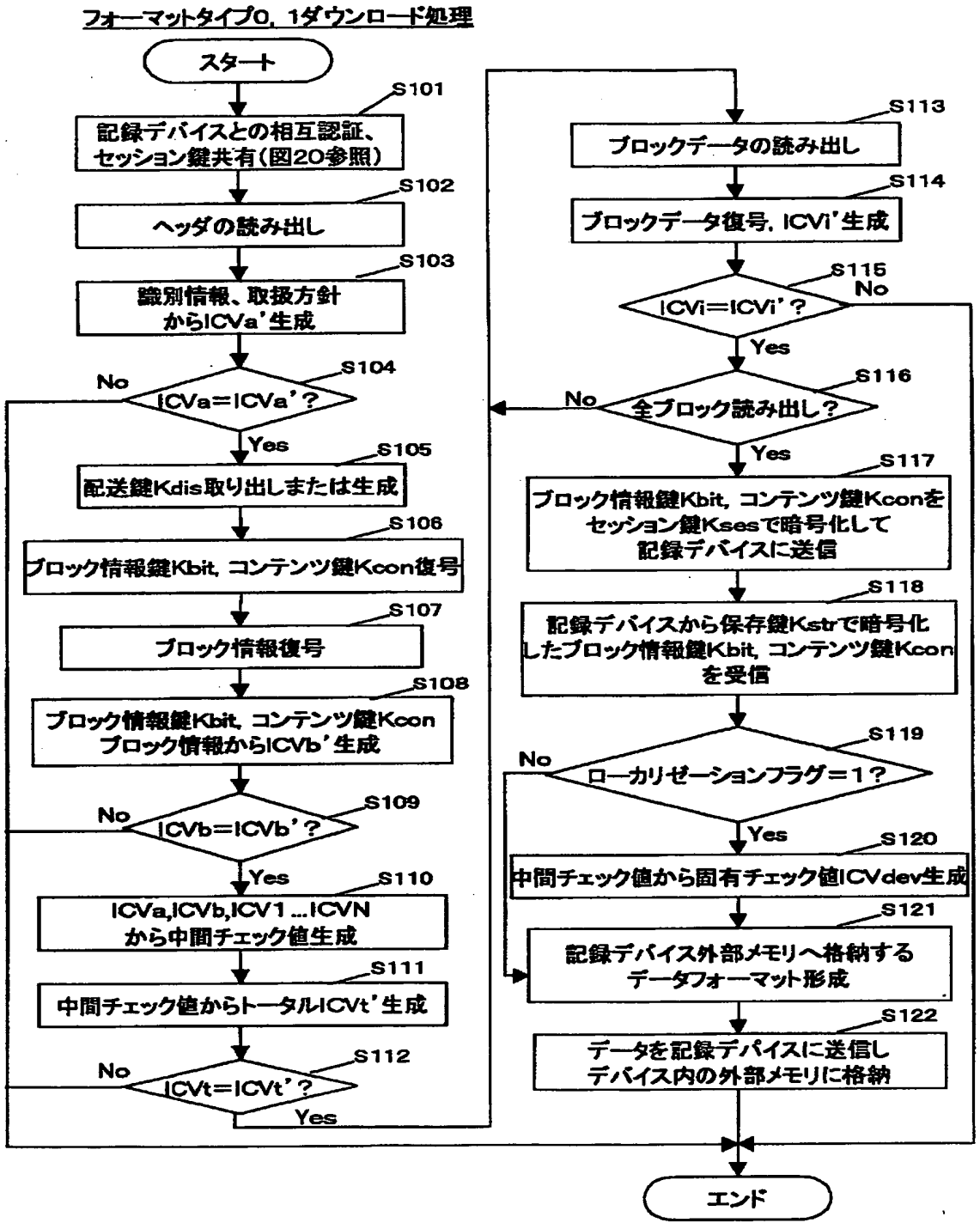
【図３７】


P−ICVI, k
(パーツkチェック値)
P−ICVI, m
(パーツmチェック値)
P−ICVI, n
(パーツnチェック値)
P−ICVI, r
(パーツrチェック値)
初期値
(Initial Value:IV)
コンテンツ
チェック値生成鍵(Kicvo)
I1
I2
I3
IN
DES
暗号化
E1
E2
E3
コンテンツチェック値: ICVi
⊕ :排他的論理和処理(8バイト単位)

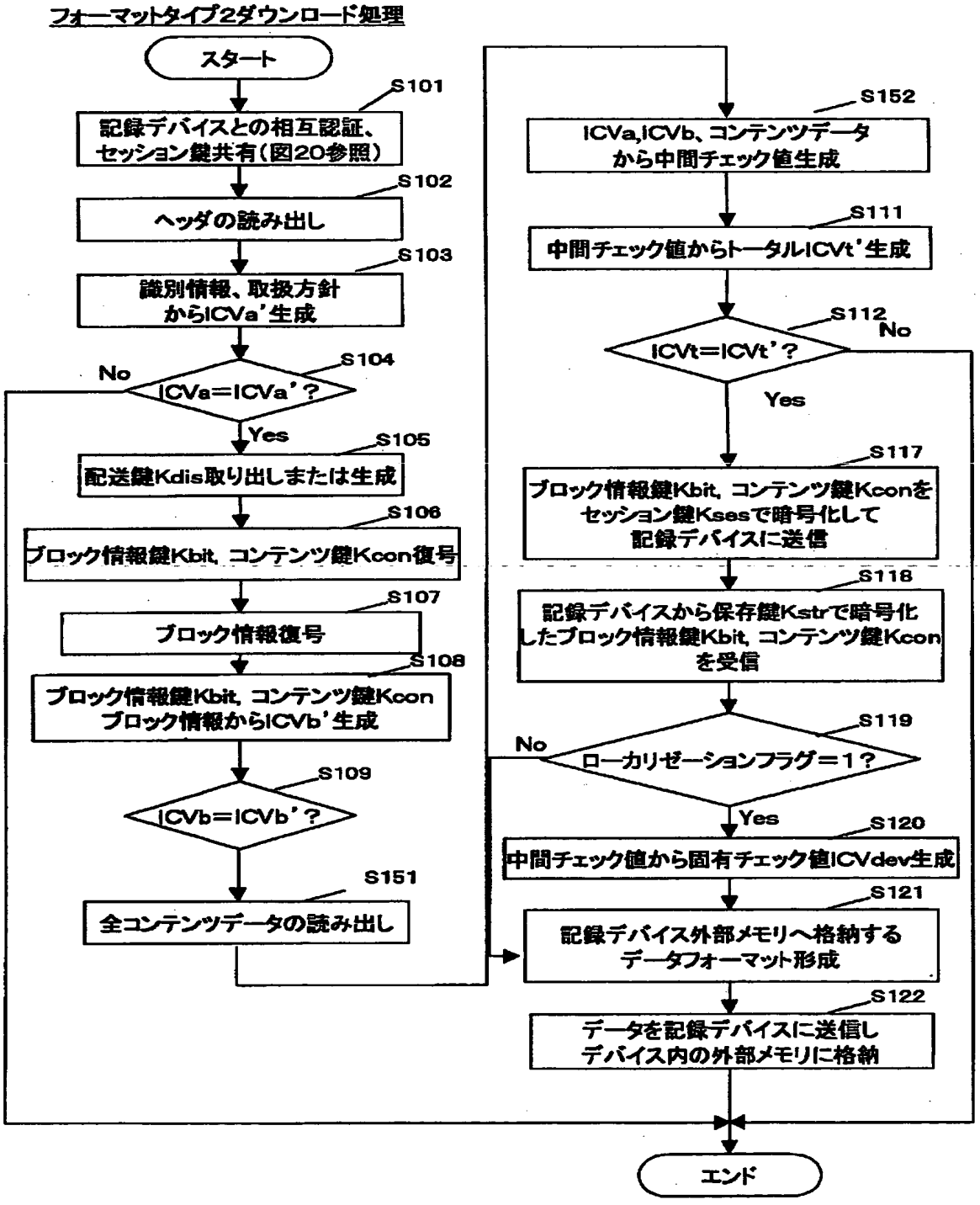
【図３８】


ICVa
(チェック値A)
ICVb
(チェック値B)
メッセージ M1
(最初の8Byte)
メッセージ MN
(最後の8Byte)
初期値
(Initial Value: IV=0
またはIV= IVt)
総チェック値生成鍵(Kicvt)
I1
I2
I3
I(N+2)
DES
暗号化
E1
E2
E3
中間チェック値: ICV
記録再生器署名鍵(Kdev)
システム署名鍵(Ksys)
総チェック値: ICVt
記録再生器固有チェック値: ICVdev
メッセージ M1～MN:コンテンツブロック1～Nのデータ
⊕ :排他的論理和処理(8バイト単位)

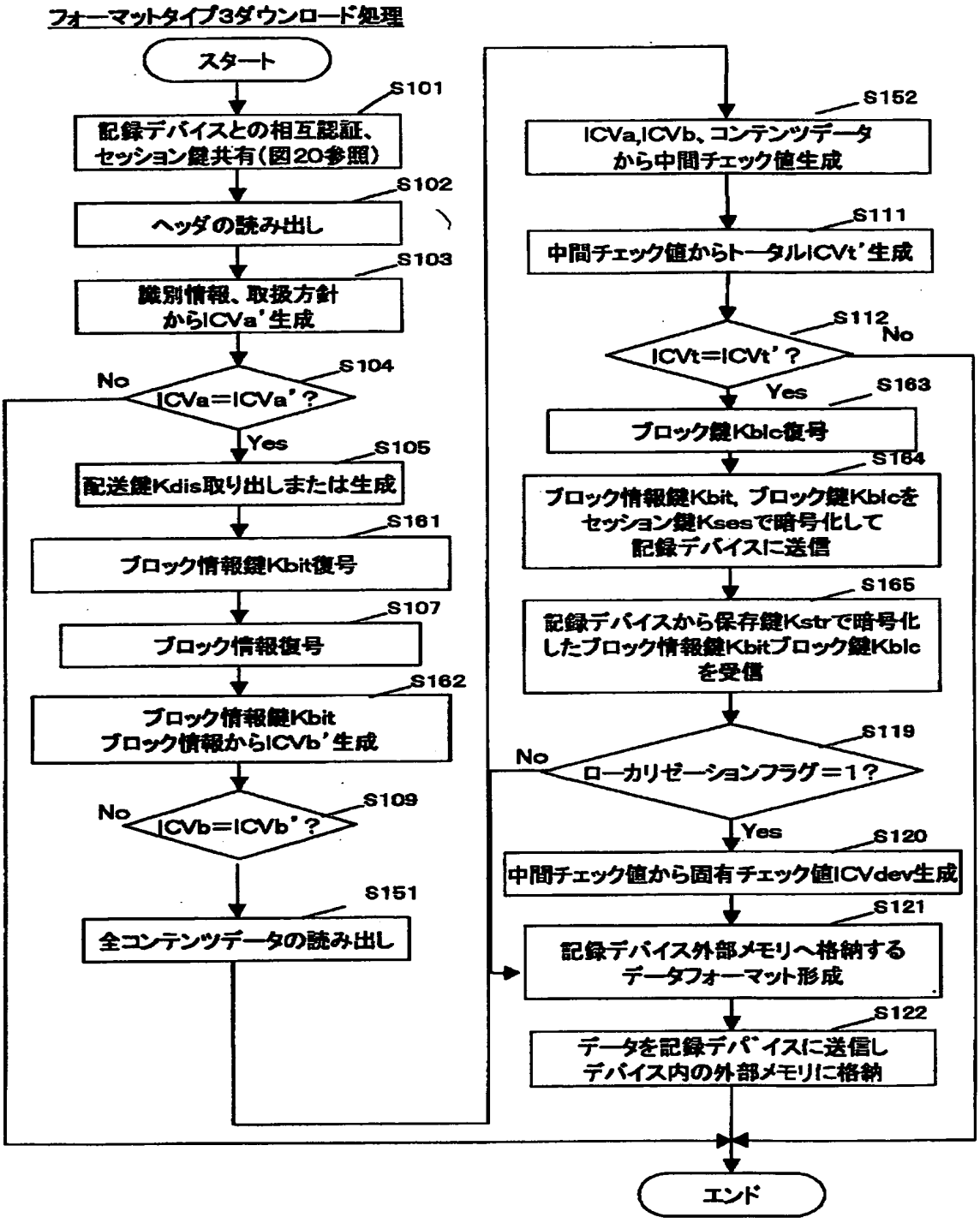
【図３９】


フォーマットタイプ0，1ダウンロード処理
スタート
S101
記録デバイスとの相互認証、セッション鍵共有(図20参照)
S102
ヘッダの読み出し
S103
識別情報、取扱方針からICVa'生成
S104
No
ICVa=ICVa'？
Yes
S105
配送鍵Kdis取り出しまたは生成
S106
ブロック情報鍵Kbit，コンテンツ鍵Kcon復号
S107
ブロック情報復号
S108
ブロック情報鍵Kbit，コンテンツ鍵Kcon
ブロック情報からICVb'生成
S109
No
ICVb=ICVb'？
Yes
S110
ICVa,ICVb,ICV1 ...ICVN
から中間チェック値生成
S111
中間チェック値からトータルICVt'生成
S112
No
ICVt=ICVt'？
Yes
S113
ブロックデータの読み出し
S114
ブロックデータ復号，ICVi'生成
S115
No
ICVi=ICVi'？
Yes
S116
No
全ブロック読み出し？
Yes
S117
ブロック情報鍵Kbit，コンテンツ鍵Kconを
セッション鍵Ksesで暗号化して
記録デバイスに送信
S118
記録デバイスから保存鍵Kstrで暗号化
したブロック情報鍵Kbit，コンテンツ鍵Kcon
を受信
S119
No
ローカリゼーションフラグ＝1？
Yes
S120
中間チェック値から固有チェック値ICVdev生成
S121
記録デバイス外部メモリへ格納する
データフォーマット形成
S122
データを記録デバイスに送信し
デバイス内の外部メモリに格納
エンド

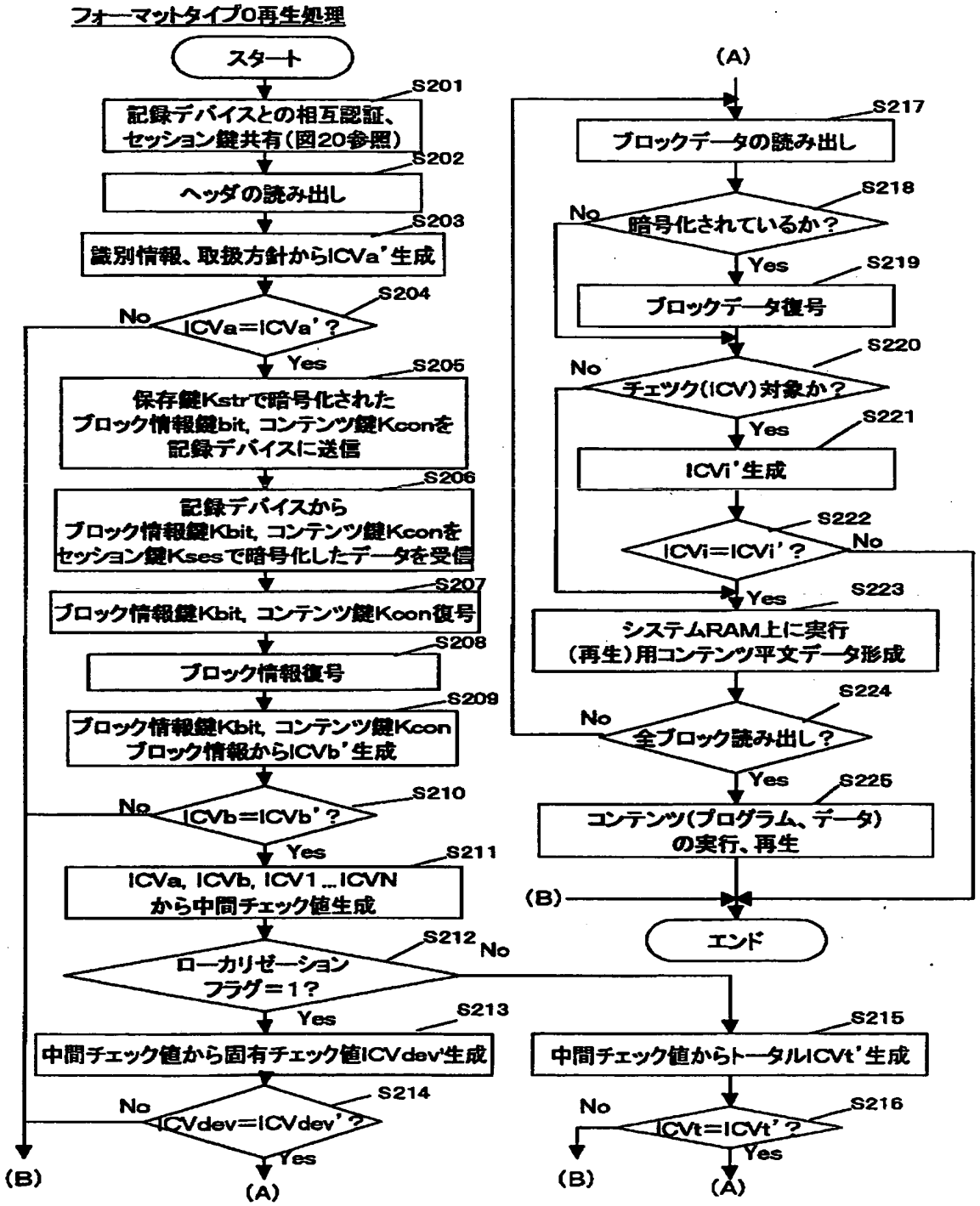
【図４０】


フォーマットタイプ2ダウンロード処理
スタート
S101
記録デバイスとの相互認証、セッション鍵共有（図20参照）
S102
ヘッダの読み出し
S103
識別情報、取扱方針からICVa'生成
S104
No
ICVa=ICVa'？
Yes
S105
配送鍵Kdis取り出しまたは生成
S106
ブロック情報鍵Kbit、コンテンツ鍵Kcon復号
S107
ブロック情報復号
S108
ブロック情報鍵Kbit、コンテンツ鍵Kconブロック情報からICVb'生成
S109
ICVb=ICVb'？
S151
全コンテンツデータの読み出し
S152
ICVa,ICVb、コンテンツデータから中間チェック値生成
S111
中間チェック値からトータルICVt'生成
S112
No
ICVt=ICVt'？
Yes
S117
ブロック情報鍵Kbit、コンテンツ鍵Kconをセッション鍵Ksesで暗号化して記録デバイスに送信
S118
記録デバイスから保存鍵Kstrで暗号化したブロック情報鍵Kbit、コンテンツ鍵Kconを受信
S119
No
ローカリゼーションフラグ＝1？
Yes
S120
中間チェック値から固有チェック値ICVdev生成
S121
記録デバイス外部メモリへ格納するデータフォーマット形成
S122
データを記録デバイスに送信しデバイス内の外部メモリに格納
エンド

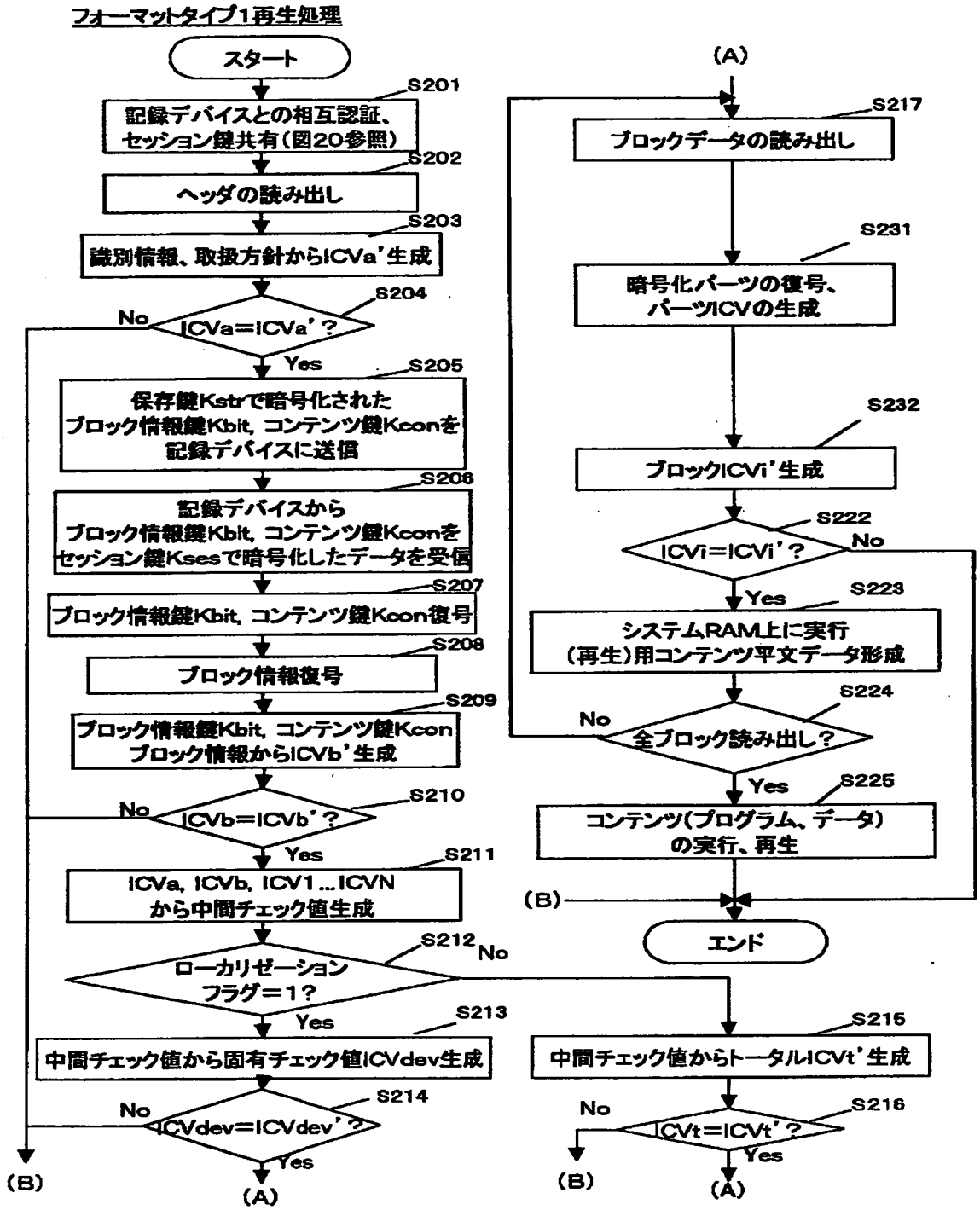
【図４１】


フォーマットタイプ3ダウンロード処理
スタート
S101
記録デバイスとの相互認証、セッション鍵共有(図20参照)
S102
ヘッダの読み出し
S103
識別情報、取扱方針からICVa'生成
S104
No
ICVa=ICVa'?
Yes
S105
配送鍵Kdis取り出しまたは生成
S161
ブロック情報鍵Kbit復号
S107
ブロック情報復号
S162
ブロック情報鍵Kbit ブロック情報からICVb'生成
S109
No
ICVb=ICVb'?
S151
全コンテンツデータの読み出し
S152
ICVa,ICVb、コンテンツデータから中間チェック値生成
S111
中間チェック値からトータルICVt'生成
S112
No
ICVt=ICVt'?
Yes
S163
ブロック鍵Kblc復号
S164
ブロック情報鍵Kbit、ブロック鍵Kblcをセッション鍵Ksesで暗号化して記録デバイスに送信
S165
記録デバイスから保存鍵Kstrで暗号化したブロック情報鍵Kbitブロック鍵Kblcを受信
S119
No
ローカリゼーションフラグ＝1?
Yes
S120
中間チェック値から固有チェック値ICVdev生成
S121
記録デバイス外部メモリへ格納するデータフォーマット形成
S122
データを記録デバイスに送信しデバイス内の外部メモリに格納
エンド

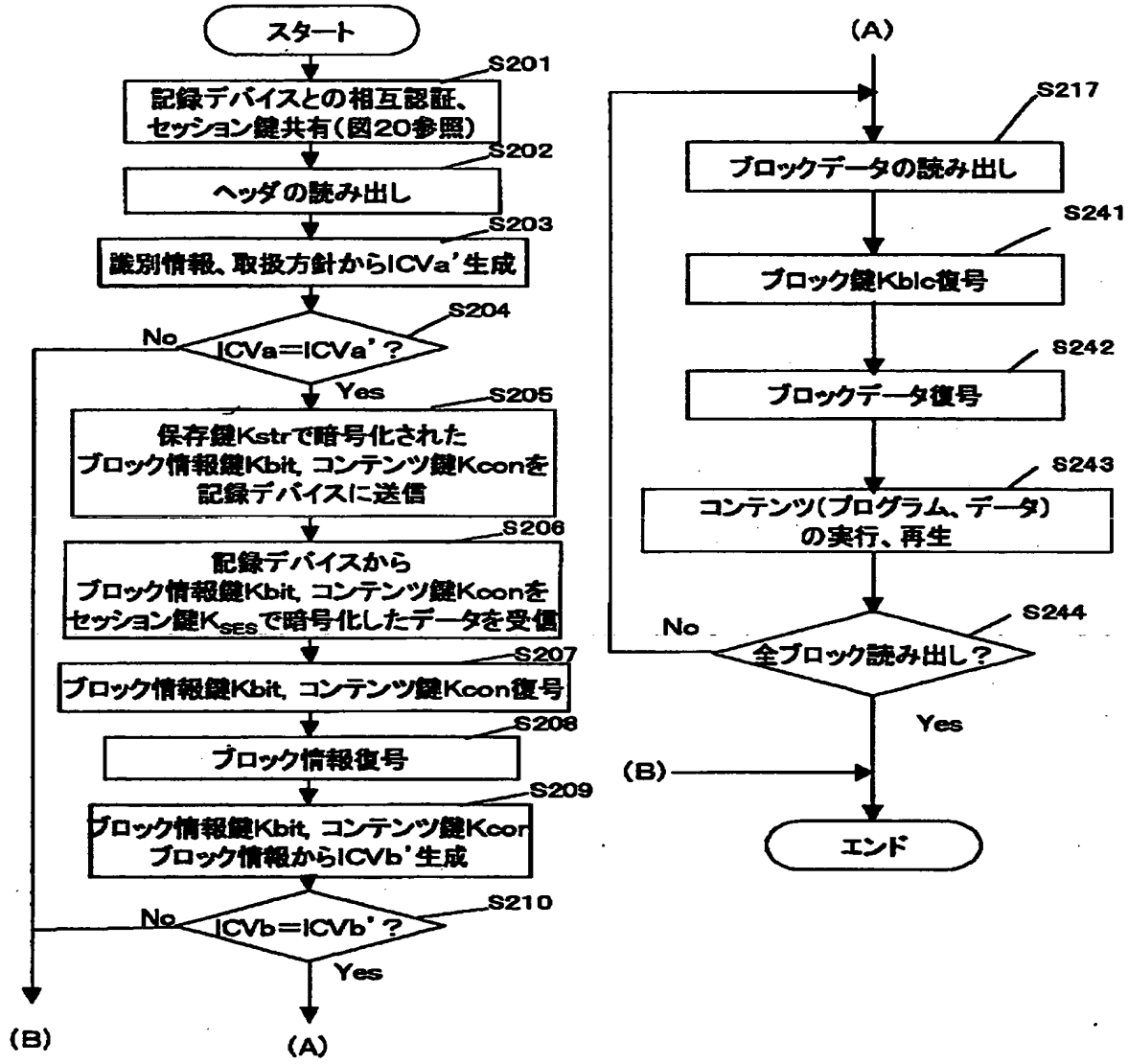
【図４２】


フォーマットタイプ0再生処理
スタート
S201
記録デバイスとの相互認証、セッション鍵共有(図20参照)
S202
ヘッダの読み出し
S203
識別情報、取扱方針からICVa'生成
S204
No
ICVa=ICVa'？
Yes
S205
保存鍵Kstrで暗号化されたブロック情報鍵bit、コンテンツ鍵Kconを記録デバイスに送信
S206
記録デバイスからブロック情報鍵Kbit、コンテンツ鍵Kconをセッション鍵Ksesで暗号化したデータを受信
S207
ブロック情報鍵Kbit、コンテンツ鍵Kcon復号
S208
ブロック情報復号
S209
ブロック情報鍵Kbit、コンテンツ鍵Kconブロック情報からICVb'生成
S210
No
ICVb=ICVb'？
Yes
S211
ICVa、ICVb、ICV1…ICVNから中間チェック値生成
S212
No
ローカリゼーションフラグ＝1？
Yes
S213
中間チェック値から固有チェック値ICVdev'生成
S214
No
ICVdev=ICVdev'？
Yes
(B)
(A)
(A)
S217
ブロックデータの読み出し
S218
No
暗号化されているか？
Yes
S219
ブロックデータ復号
S220
No
チェック(ICV)対象か？
Yes
S221
ICVi'生成
S222
ICVi=ICVi'？
No
Yes
S223
システムRAM上に実行(再生)用コンテンツ平文データ形成
S224
No
全ブロック読み出し？
Yes
S225
コンテンツ(プログラム、データ)の実行、再生
(B)
エンド
S215
中間チェック値からトータルICVt'生成
S216
No
ICVt=ICVt'？
Yes
(B)
(A)

【図４３】

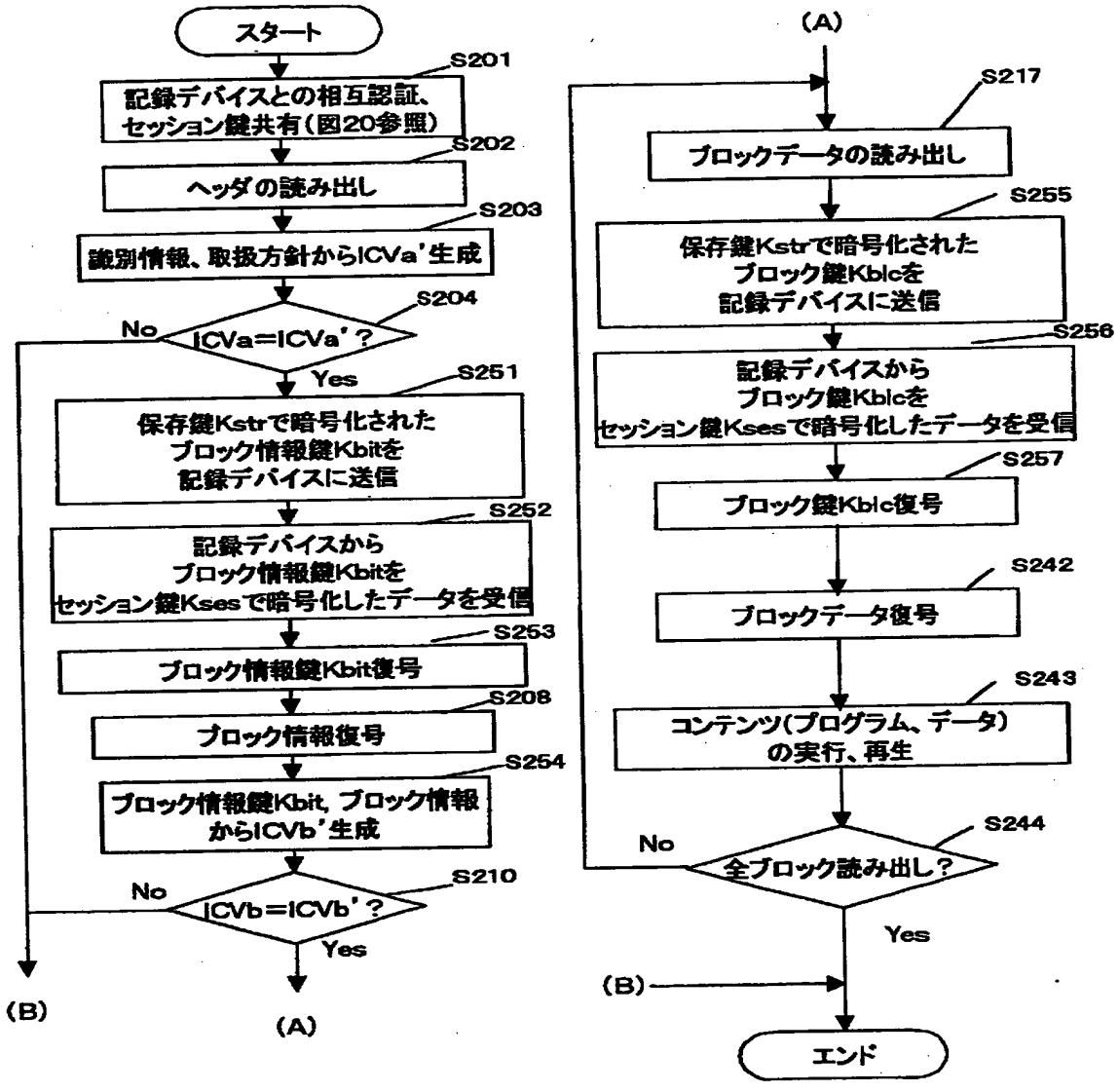

フォーマットタイプ1再生処理
スタート
S201
記録デバイスとの相互認証、セッション鍵共有(図20参照)
S202
ヘッダの読み出し
S203
識別情報、取扱方針からICVa'生成
S204
No
ICVa=ICVa'?
Yes
S205
保存鍵Kstrで暗号化されたブロック情報鍵Kbit, コンテンツ鍵Kconを記録デバイスに送信
S206
記録デバイスからブロック情報鍵Kbit, コンテンツ鍵Kconをセッション鍵Ksesで暗号化したデータを受信
S207
ブロック情報鍵Kbit, コンテンツ鍵Kcon復号
S208
ブロック情報復号
S209
ブロック情報鍵Kbit, コンテンツ鍵Kconブロック情報からICVb'生成
S210
No
ICVb=ICVb'?
Yes
S211
ICVa, ICVb, ICV1...ICVNから中間チェック値生成
S212
No
ローカリゼーションフラグ=1?
Yes
S213
中間チェック値から固有チェック値ICVdev生成
S214
No
ICVdev=ICVdev'?
Yes
(B)
(A)
(A)
S217
ブロックデータの読み出し
S231
暗号化パーツの復号、パーツICVの生成
S232
ブロックICVi'生成
S222
ICVi=ICVi'?
No
Yes
S223
システムRAM上に実行(再生)用コンテンツ平文データ形成
S224
No
全ブロック読み出し?
Yes
S225
コンテンツ(プログラム、データ)の実行、再生
(B)
エンド
S215
中間チェック値からトータルICVt'生成
S216
No
ICVt=ICVt'?
Yes
(B)
(A)

【図４４】

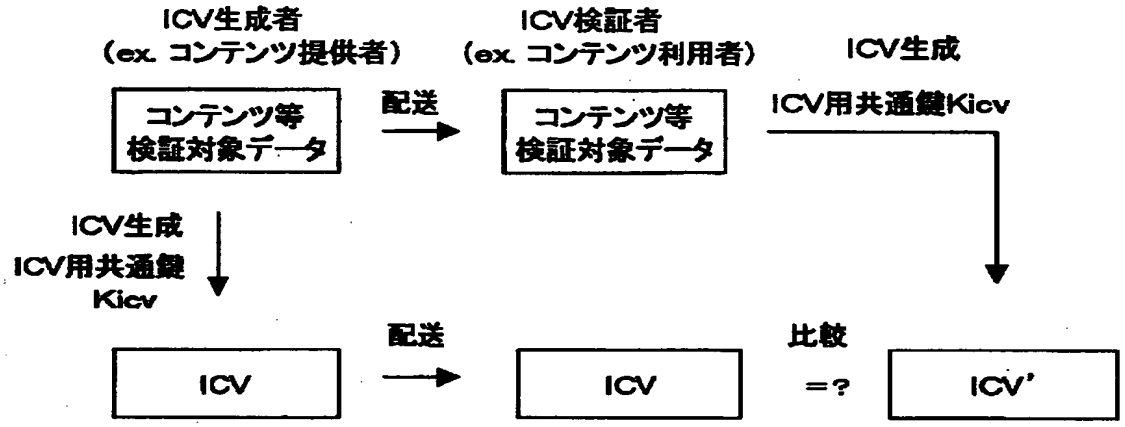

スタート
S201
記録デバイスとの相互認証、
セッション鍵共有(図20参照)
S202
ヘッダの読み出し
S203
識別情報、取扱方針からICVa'生成
S204
No
ICVa=ICVa'？
Yes
S205
保存鍵Kstrで暗号化された
ブロック情報鍵Kbit, コンテンツ鍵Kconを
記録デバイスに送信
S206
記録デバイスから
ブロック情報鍵Kbit, コンテンツ鍵Kconを
セッション鍵K_{SES}で暗号化したデータを受信
S207
ブロック情報鍵Kbit, コンテンツ鍵Kcon復号
S208
ブロック情報復号
S209
ブロック情報鍵Kbit, コンテンツ鍵Kcon
ブロック情報からICVb'生成
S210
No
ICVb=ICVb'？
Yes
(B)
(A)
(A)
S217
ブロックデータの読み出し
S241
ブロック鍵Kblc復号
S242
ブロックデータ復号
S243
コンテンツ(プログラム、データ)
の実行、再生
S244
No
全ブロック読み出し？
Yes
(B)
エンド

【図４５】

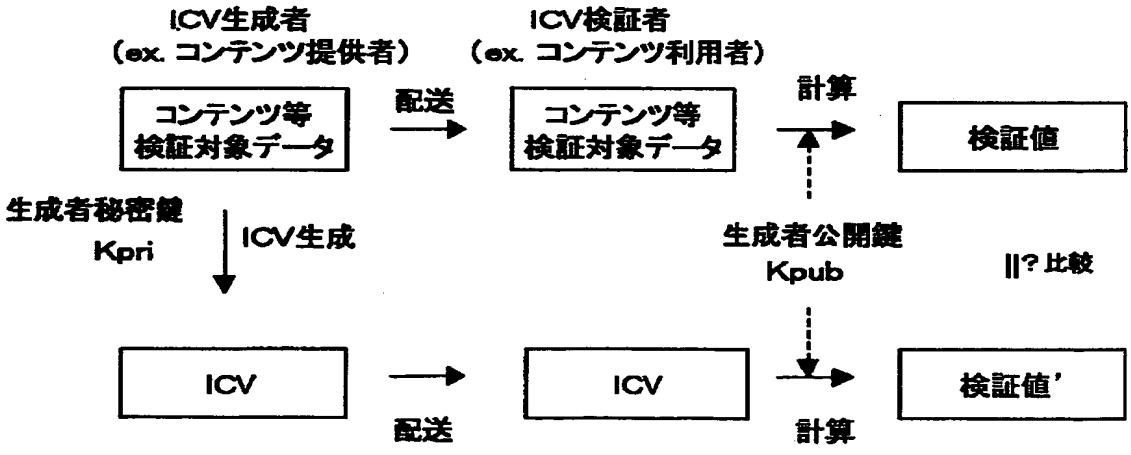
フォーマットタイプ3再生処理



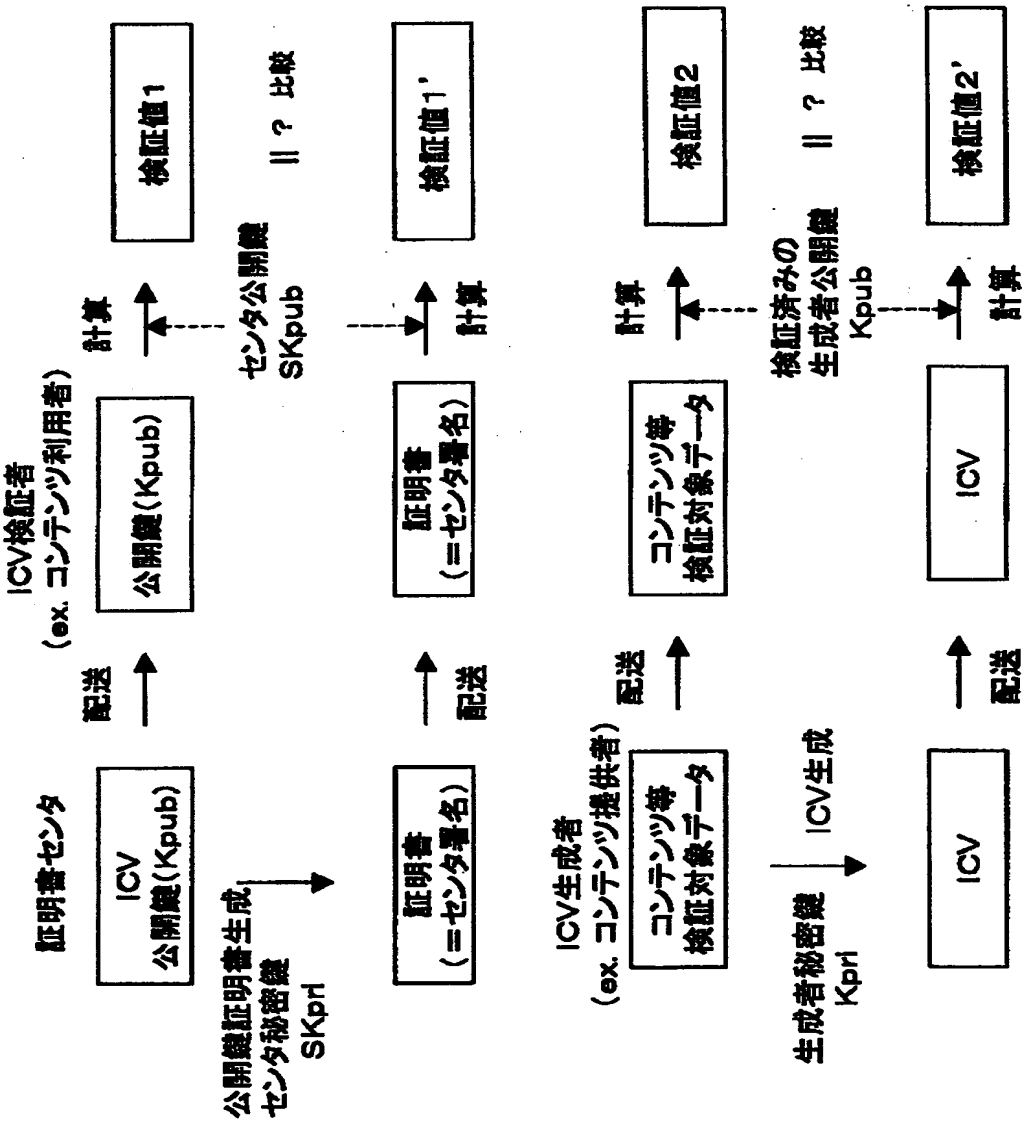
【図４６】


ICV生成者
(ex. コンテンツ提供者)
ICV検証者
(ex. コンテンツ利用者)
ICV生成
コンテンツ等
検証対象データ
配送
コンテンツ等
検証対象データ
ICV用共通鍵Kicv
ICV生成
ICV用共通鍵
Kicv
配送
比較
ICV
ICV
=?
ICV'

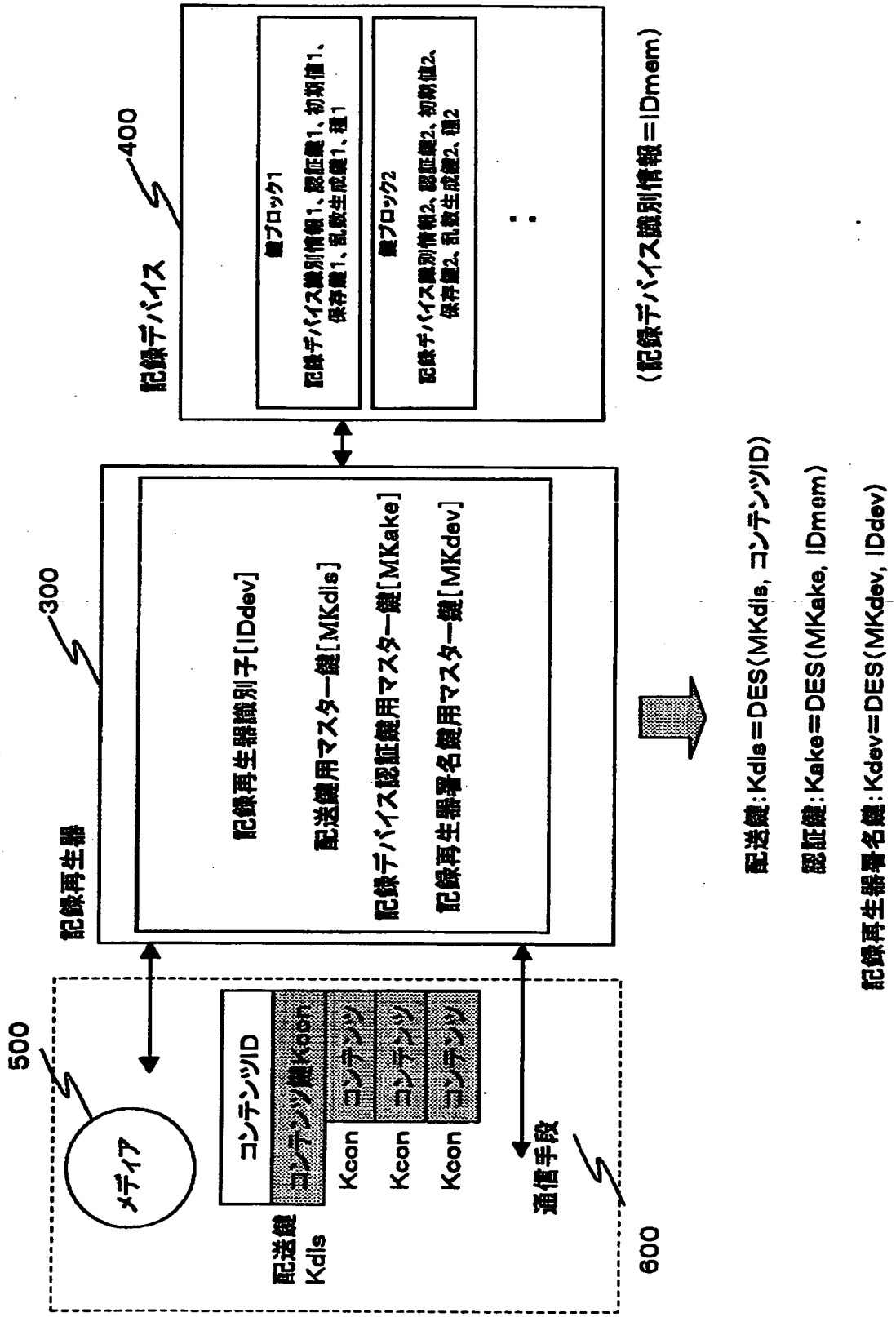
【図４７】


ICV生成者
(ex. コンテンツ提供者)
ICV検証者
(ex. コンテンツ利用者)
コンテンツ等
検証対象データ
配送
コンテンツ等
検証対象データ
計算
検証値
生成者秘密鍵
Kpri
ICV生成
生成者公開鍵
Kpub
II? 比較
ICV
ICV
検証値'
配送
計算

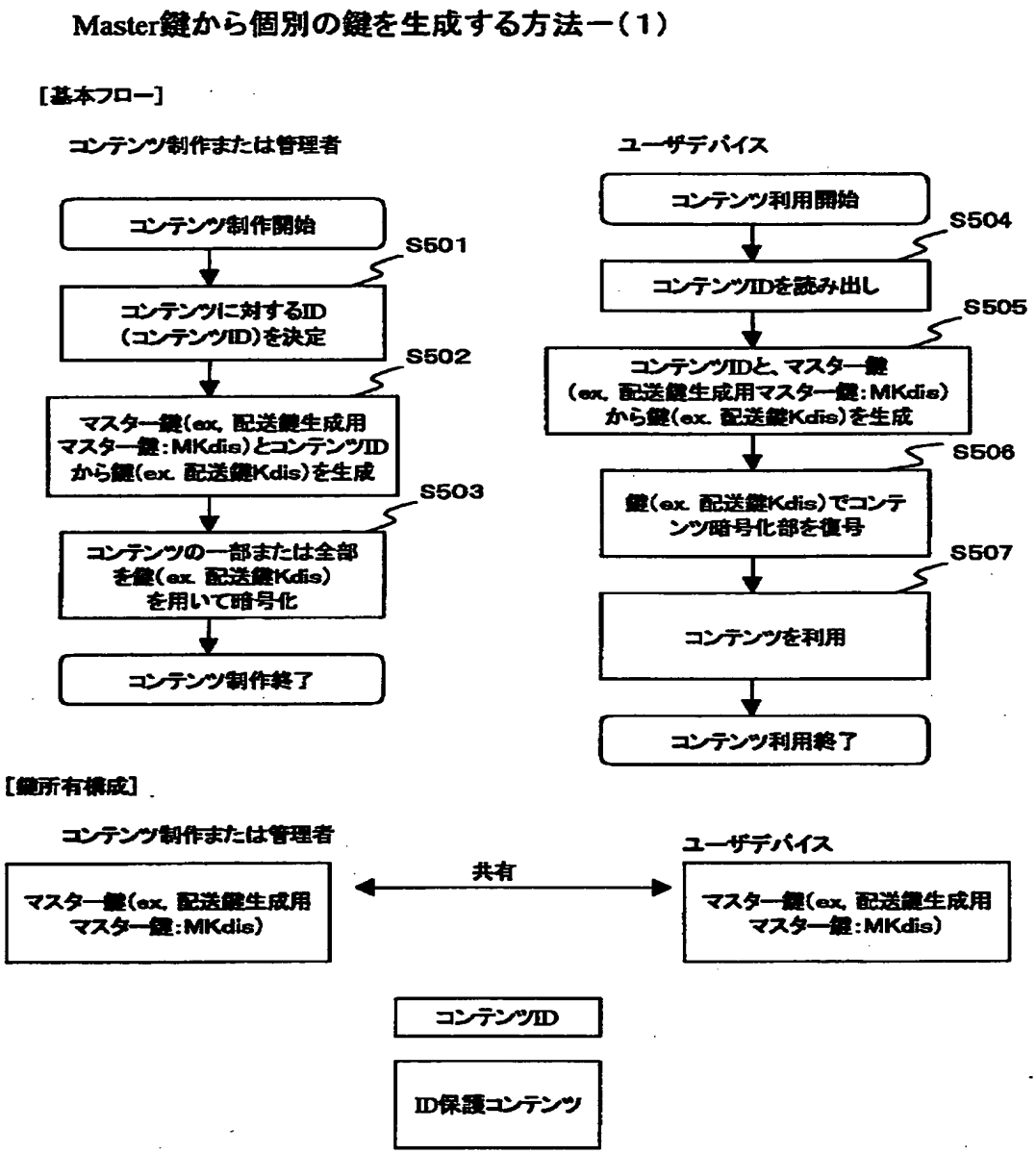
【図４８】


証明書センタ
ICV
公開鍵(Kpub)
配送
ICV検証者
(ex. コンテンツ利用者)
公開鍵
(Kpub)
計算
検証値1
センタ公開鍵
SKpub
＝？ 比較
公開鍵証明書生成
センタ秘密鍵
SKpri
証明書
(＝センタ署名)
配送
証明書
(＝センタ署名)
計算
検証値1'
ICV生成者
(ex. コンテンツ提供者)
コンテンツ等
検証対象データ
配送
コンテンツ等
検証対象データ
計算
検証値2
生成者秘密鍵
Kpri
ICV生成
ICV
配送
ICV
検証済みの
生成者公開鍵
Kpub
＝？ 比較
計算
検証値2'

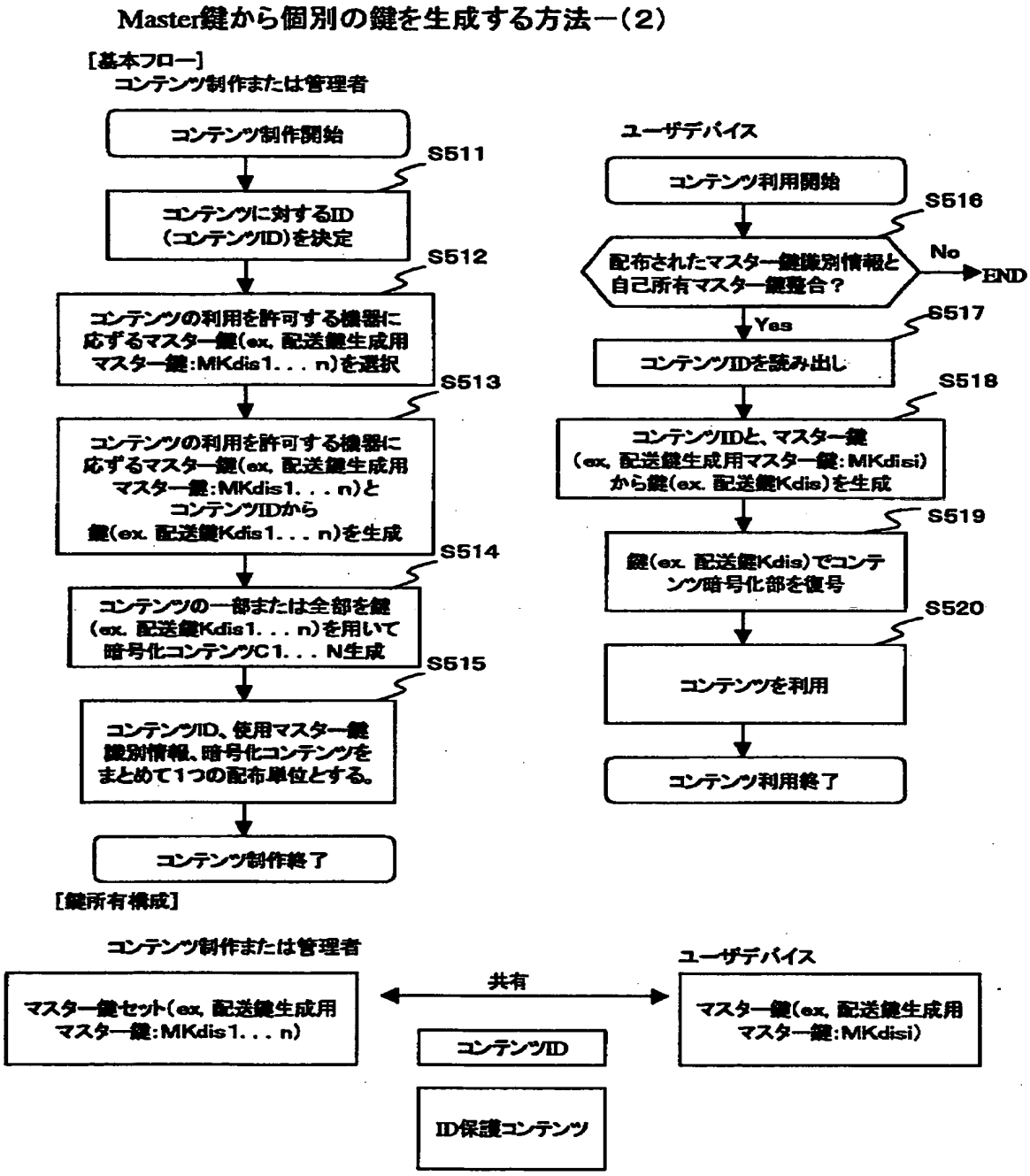
【図４９】


400
記録デバイス
鍵ブロック1
記録デバイス識別情報1、認証鍵1、初期値1、保存鍵1、乱数生成鍵1、種1
鍵ブロック2
記録デバイス識別情報2、認証鍵2、初期値2、保存鍵2、乱数生成鍵2、種2
(記録デバイス識別情報=IDmem)
300
記録再生器
記録再生器識別子[IDdev]
配送鍵用マスター鍵[MKdis]
記録デバイス認証鍵用マスター鍵[MKake]
記録再生器署名鍵用マスター鍵[MKdev]
配送鍵:Kdis=DES(MKdis, コンテンツID)
認証鍵:Kake=DES(MKake, IDmem)
記録再生器署名鍵:Kdev=DES(MKdev, IDdev)
500
メディア
コンテンツID
コンテンツ鍵Kcon
コンテンツ
コンテンツ
コンテンツ
Kcon
Kcon
Kcon
配送鍵
Kdis
通信手段
600

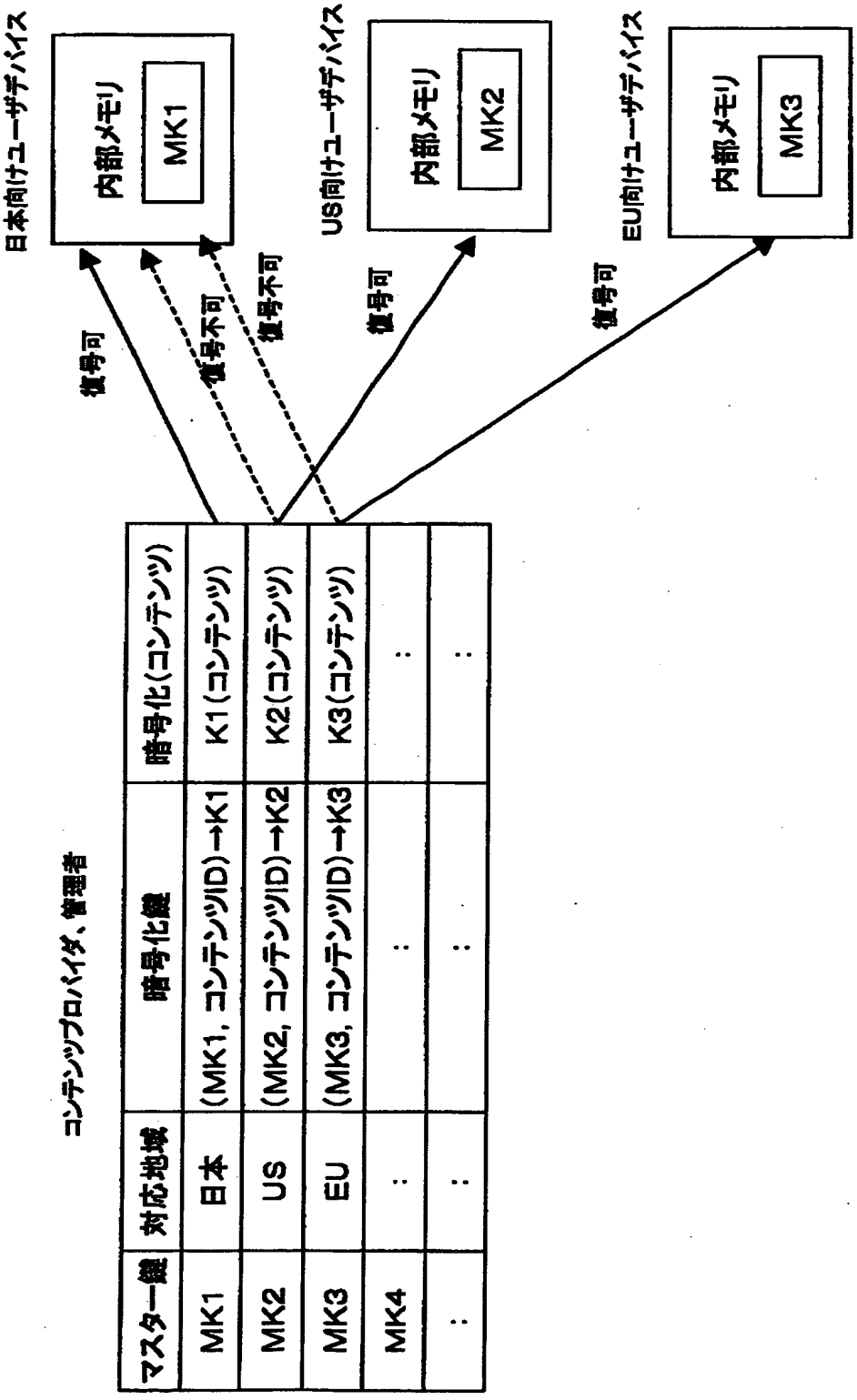
【図５０】


Master鍵から個別の鍵を生成する方法－(1)
[基本フロー]
コンテンツ制作または管理者
コンテンツ制作開始
S501
コンテンツに対するID
(コンテンツID)を決定
S502
マスター鍵(ex. 配送鍵生成用
マスター鍵:MKdis)とコンテンツID
から鍵(ex. 配送鍵Kdis)を生成
S503
コンテンツの一部または全部
を鍵(ex. 配送鍵Kdis)
を用いて暗号化
コンテンツ制作終了
ユーザデバイス
コンテンツ利用開始
S504
コンテンツIDを読み出し
S505
コンテンツIDと、マスター鍵
(ex. 配送鍵生成用マスター鍵:MKdis)
から鍵(ex. 配送鍵Kdis)を生成
S506
鍵(ex. 配送鍵Kdis)でコンテ
ンツ暗号化部を復号
S507
コンテンツを利用
コンテンツ利用終了
[鍵所有構成]
コンテンツ制作または管理者
マスター鍵(ex. 配送鍵生成用
マスター鍵:MKdis)
共有
ユーザデバイス
マスター鍵(ex. 配送鍵生成用
マスター鍵:MKdis)
コンテンツID
ID保護コンテンツ

【図５１】

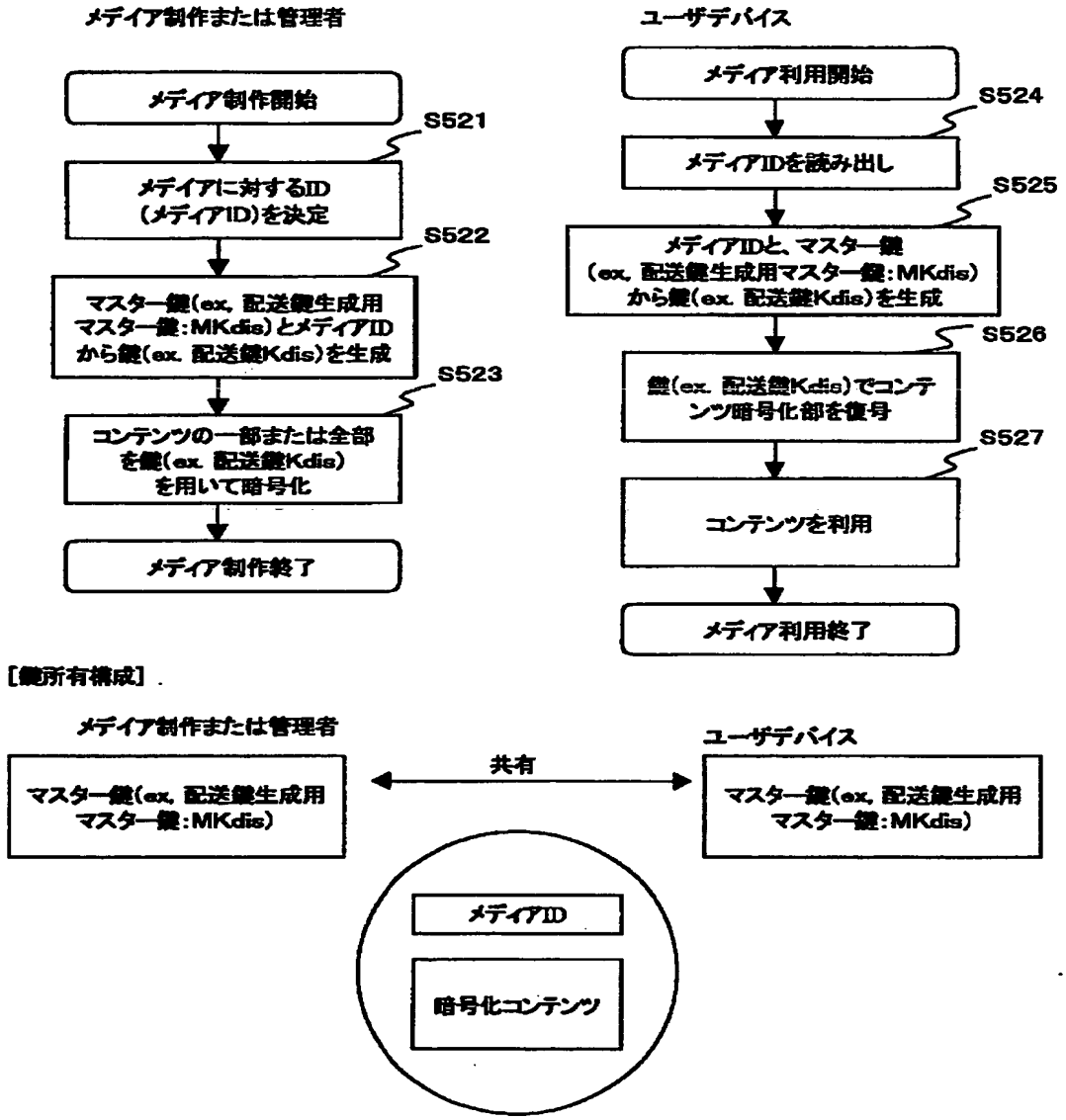

Master鍵から個別の鍵を生成する方法－(2)
[基本フロー]
コンテンツ制作または管理者
コンテンツ制作開始
S511
コンテンツに対するID
(コンテンツID)を決定
S512
コンテンツの利用を許可する機器に
応ずるマスター鍵(ex. 配送鍵生成用
マスター鍵:MKdis1. . . n)を選択
S513
コンテンツの利用を許可する機器に
応ずるマスター鍵(ex. 配送鍵生成用
マスター鍵:MKdis1. . . n)と
コンテンツIDから
鍵(ex. 配送鍵Kdis1. . . n)を生成
S514
コンテンツの一部または全部を鍵
(ex. 配送鍵Kdis1. . . n)を用いて
暗号化コンテンツC1. . . N生成
S515
コンテンツID、使用マスター鍵
識別情報、暗号化コンテンツを
まとめて1つの配布単位とする。
コンテンツ制作終了
ユーザデバイス
コンテンツ利用開始
S516
配布されたマスター鍵識別情報と
自己所有マスター鍵整合？
No
END
Yes
S517
コンテンツIDを読み出し
S518
コンテンツIDと、マスター鍵
(ex. 配送鍵生成用マスター鍵:MKdisi)
から鍵(ex. 配送鍵Kdis)を生成
S519
鍵(ex. 配送鍵Kdis)でコンテ
ンツ暗号化部を復号
S520
コンテンツを利用
コンテンツ利用終了
[鍵所有構成]
コンテンツ制作または管理者
マスター鍵セット(ex. 配送鍵生成用
マスター鍵:MKdis1. . . n)
共有
ユーザデバイス
マスター鍵(ex. 配送鍵生成用
マスター鍵:MKdisi)
コンテンツID
ID保護コンテンツ

【図５２】

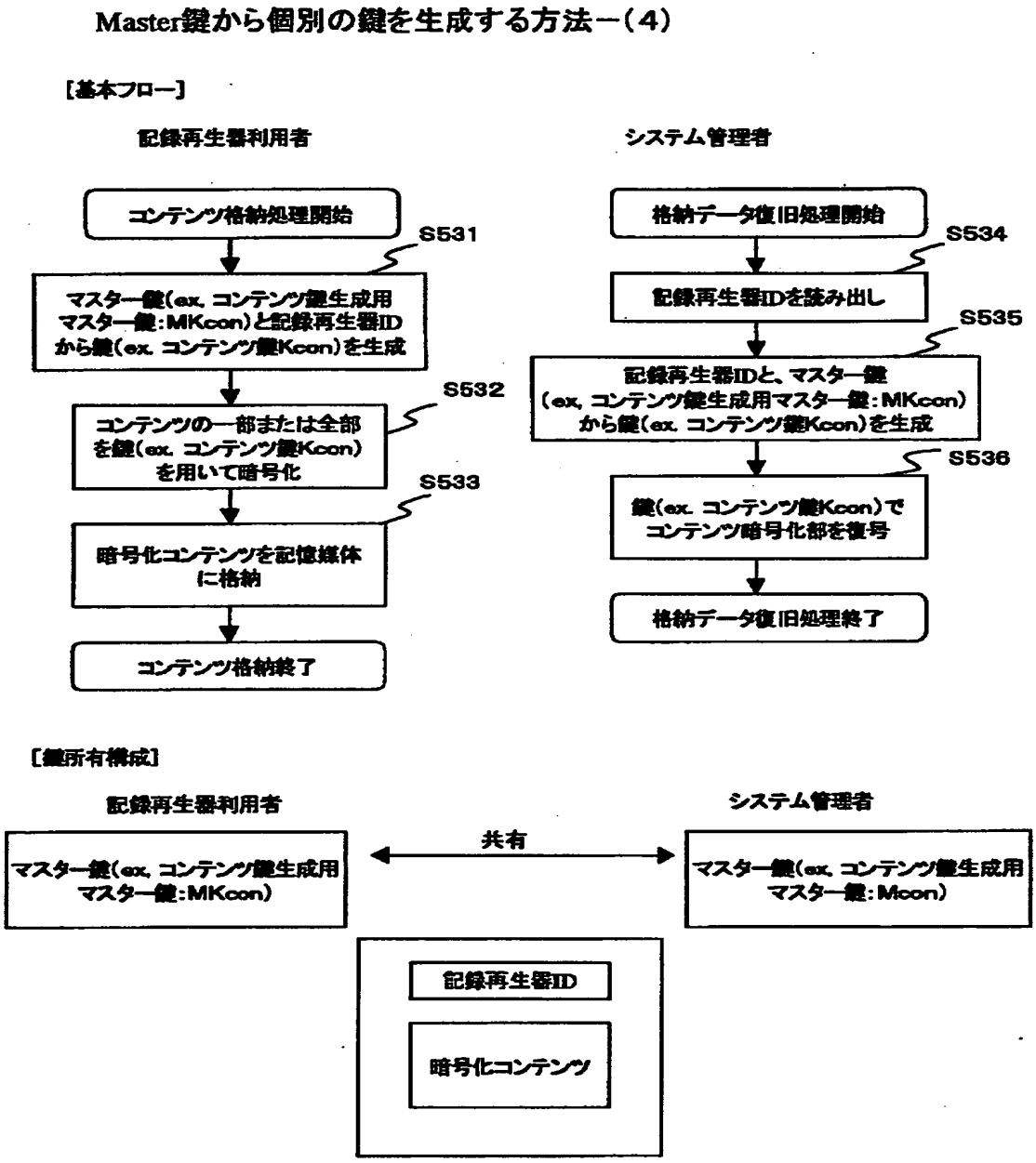

日本向けユーザデバイス
内部メモリ
MK1
US向けユーザデバイス
内部メモリ
MK2
EU向けユーザデバイス
内部メモリ
MK3
復号可
復号不可
復号不可
復号可
復号可
コンテンツプロバイダ、管理者
マスター鍵
対応地域
暗号化鍵
暗号化(コンテンツ)
MK1
日本
(MK1, コンテンツID)→K1
K1(コンテンツ)
MK2
US
(MK2, コンテンツID)→K2
K2(コンテンツ)
MK3
EU
(MK3, コンテンツID)→K3
K3(コンテンツ)
MK4

【図５３】

Master鍵から個別の鍵を生成する方法－(3)



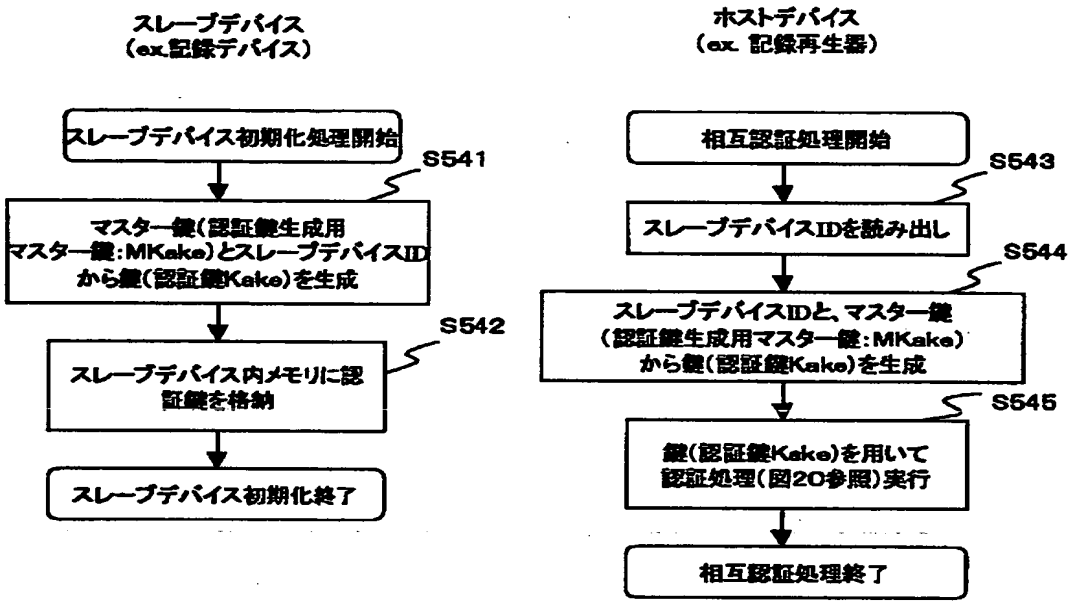
【図５４】


Master鍵から個別の鍵を生成する方法－(4)
【基本フロー】
記録再生器利用者
システム管理者
コンテンツ格納処理開始
S531
マスター鍵(ex. コンテンツ鍵生成用マスター鍵:MKcon)と記録再生器IDから鍵(ex. コンテンツ鍵Kcon)を生成
S532
コンテンツの一部または全部を鍵(ex. コンテンツ鍵Kcon)を用いて暗号化
S533
暗号化コンテンツを記憶媒体に格納
コンテンツ格納終了
格納データ復旧処理開始
S534
記録再生器IDを読み出し
S535
記録再生器IDと、マスター鍵(ex. コンテンツ鍵生成用マスター鍵:MKcon)から鍵(ex. コンテンツ鍵Kcon)を生成
S536
鍵(ex. コンテンツ鍵Kcon)でコンテンツ暗号化部を復号
格納データ復旧処理終了
【鍵所有構成】
記録再生器利用者
システム管理者
マスター鍵(ex. コンテンツ鍵生成用マスター鍵:MKcon)
共有
マスター鍵(ex. コンテンツ鍵生成用マスター鍵:Mcon)
記録再生器ID
暗号化コンテンツ

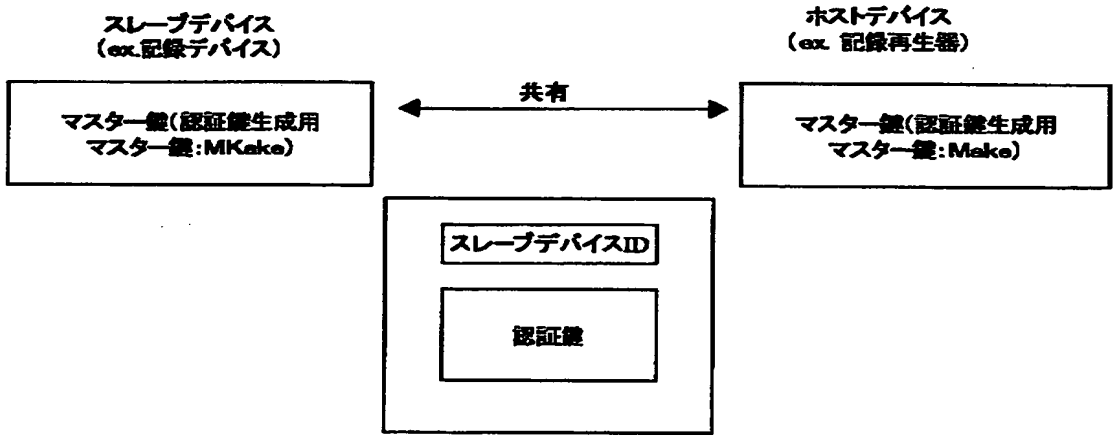
【図５５】

Master鍵から個別の鍵を生成する方法－(5)

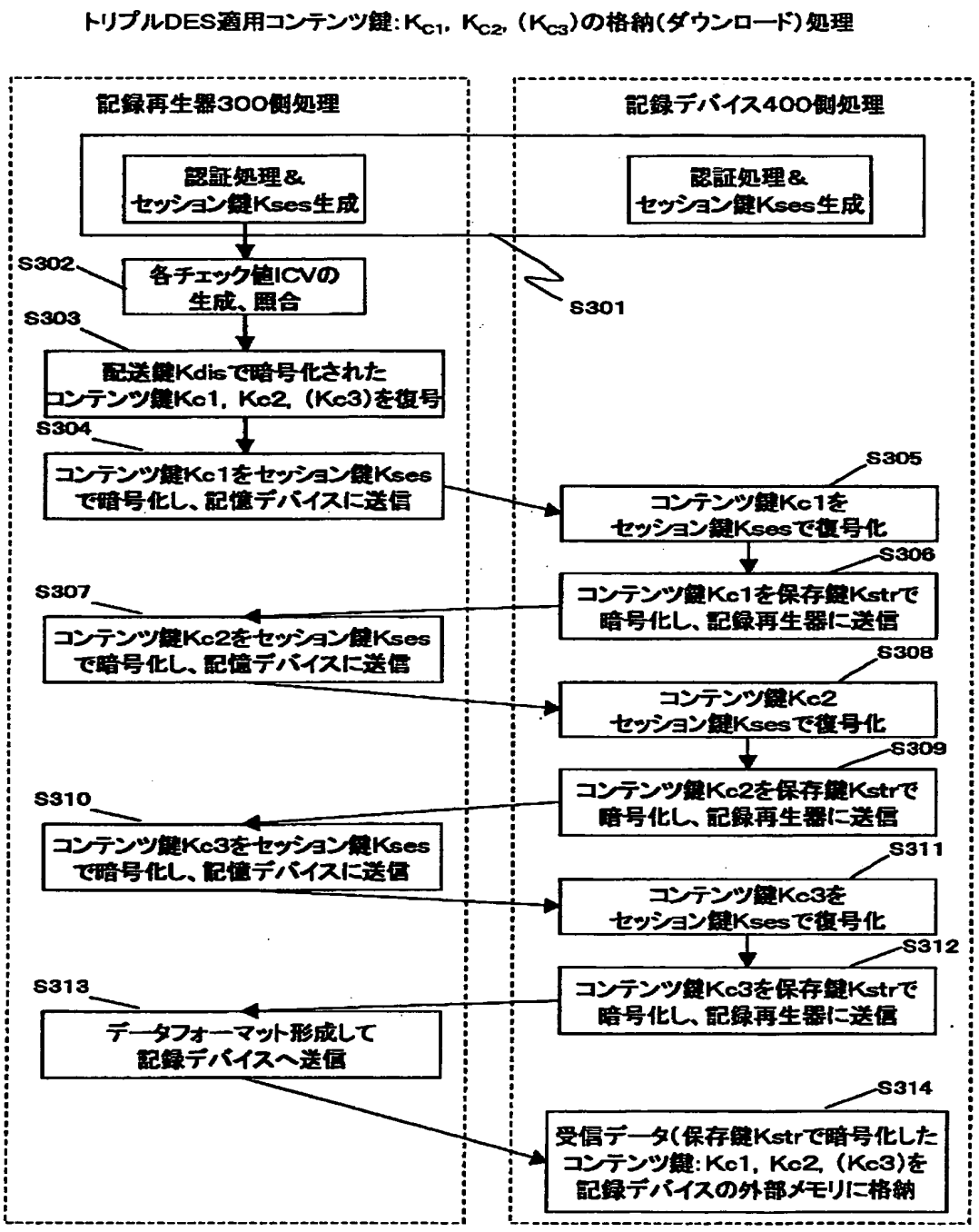
[基本フロー]



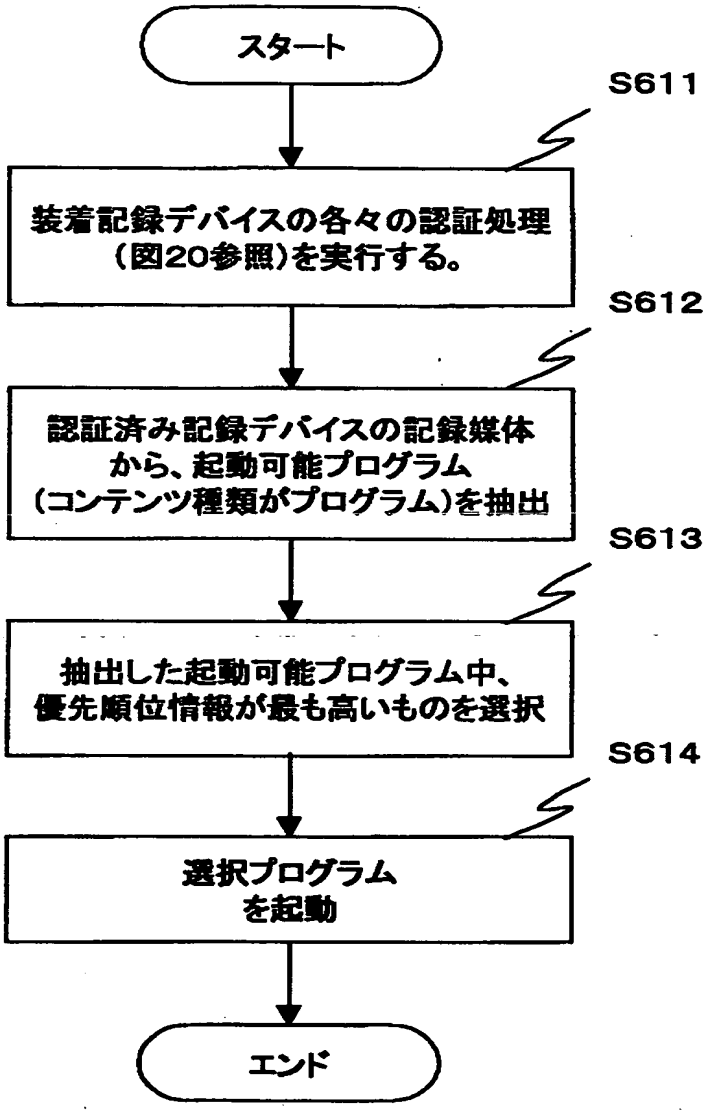
[鍵所有構成]



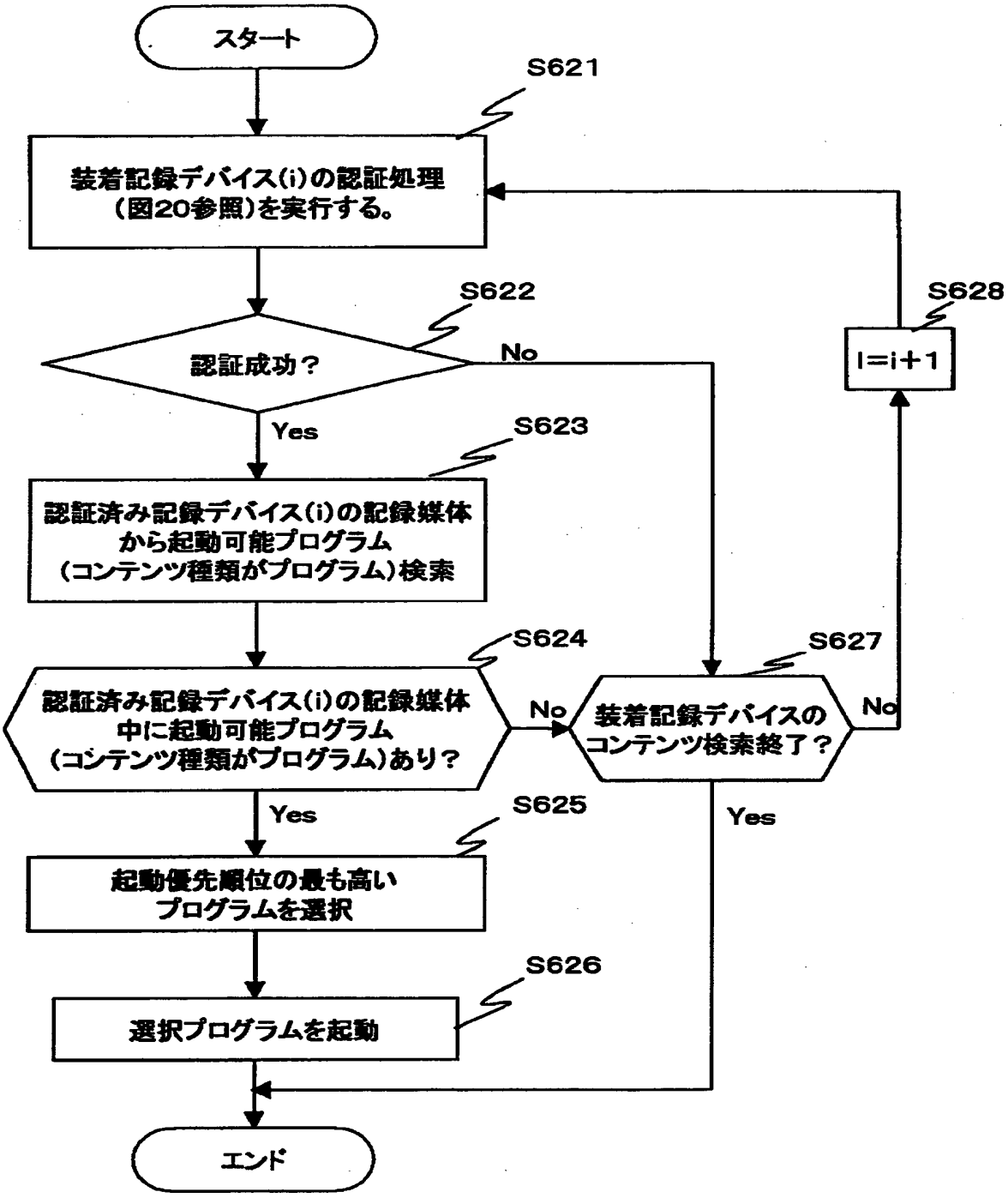
【図５６】


トリプルDES適用コンテンツ鍵:K_{c1}, K_{c2}, (K_{c3})の格納(ダウンロード)処理
記録再生器300側処理
記録デバイス400側処理
認証処理&
セッション鍵Kses生成
認証処理&
セッション鍵Kses生成
S301
S302
各チェック値ICVの
生成、照合
S303
配送鍵Kdisで暗号化された
コンテンツ鍵Kc1, Kc2, (Kc3)を復号
S304
コンテンツ鍵Kc1をセッション鍵Ksesで暗号化し、記憶デバイスに送信
S305
コンテンツ鍵Kc1を
セッション鍵Ksesで復号化
S306
コンテンツ鍵Kc1を保存鍵Kstrで
暗号化し、記録再生器に送信
S307
コンテンツ鍵Kc2をセッション鍵Ksesで暗号化し、記憶デバイスに送信
S308
コンテンツ鍵Kc2
セッション鍵Ksesで復号化
S309
コンテンツ鍵Kc2を保存鍵Kstrで
暗号化し、記録再生器に送信
S310
コンテンツ鍵Kc3をセッション鍵Ksesで暗号化し、記憶デバイスに送信
S311
コンテンツ鍵Kc3を
セッション鍵Ksesで復号化
S312
コンテンツ鍵Kc3を保存鍵Kstrで
暗号化し、記録再生器に送信
S313
データフォーマット形成して
記録デバイスへ送信
S314
受信データ(保存鍵Kstrで暗号化した
コンテンツ鍵:Kc1, Kc2, (Kc3)を
記録デバイスの外部メモリに格納

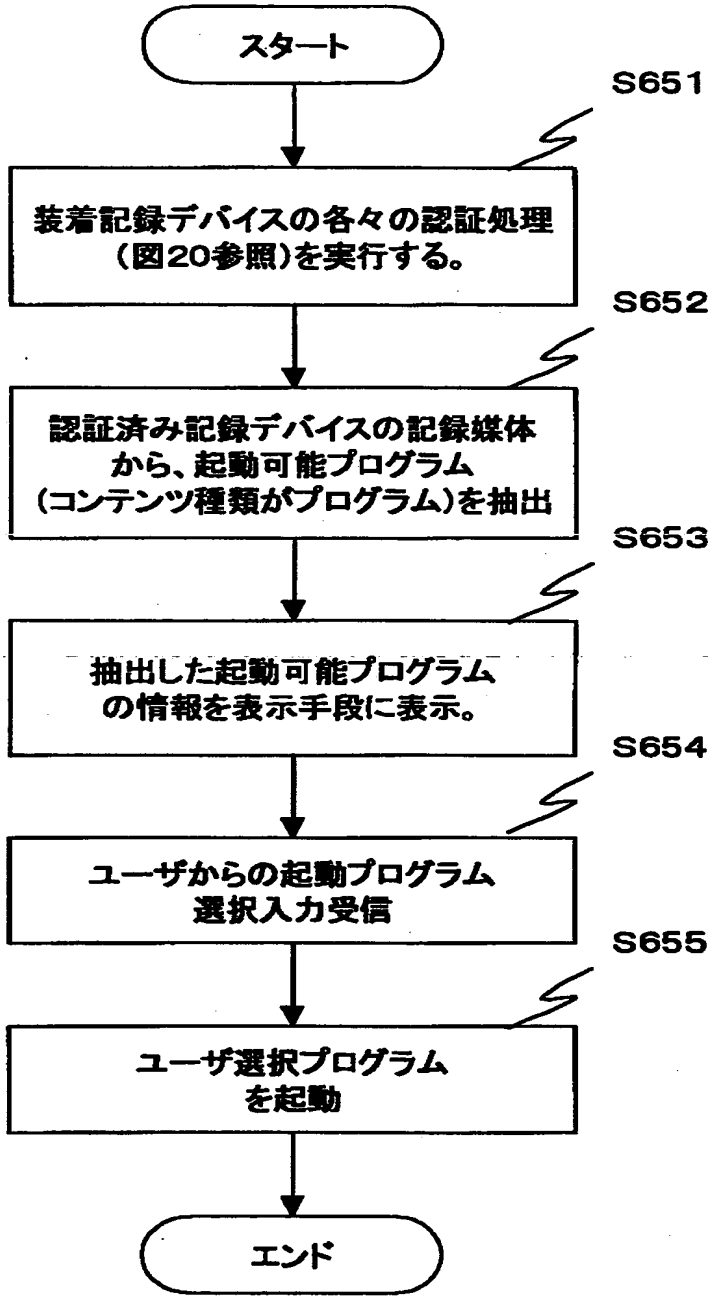
【図５７】


スタート
S611
装着記録デバイスの各々の認証処理
（図20参照）を実行する。
S612
認証済み記録デバイスの記録媒体
から、起動可能プログラム
（コンテンツ種類がプログラム）を抽出
S613
抽出した起動可能プログラム中、
優先順位情報が最も高いものを選択
S614
選択プログラム
を起動
エンド

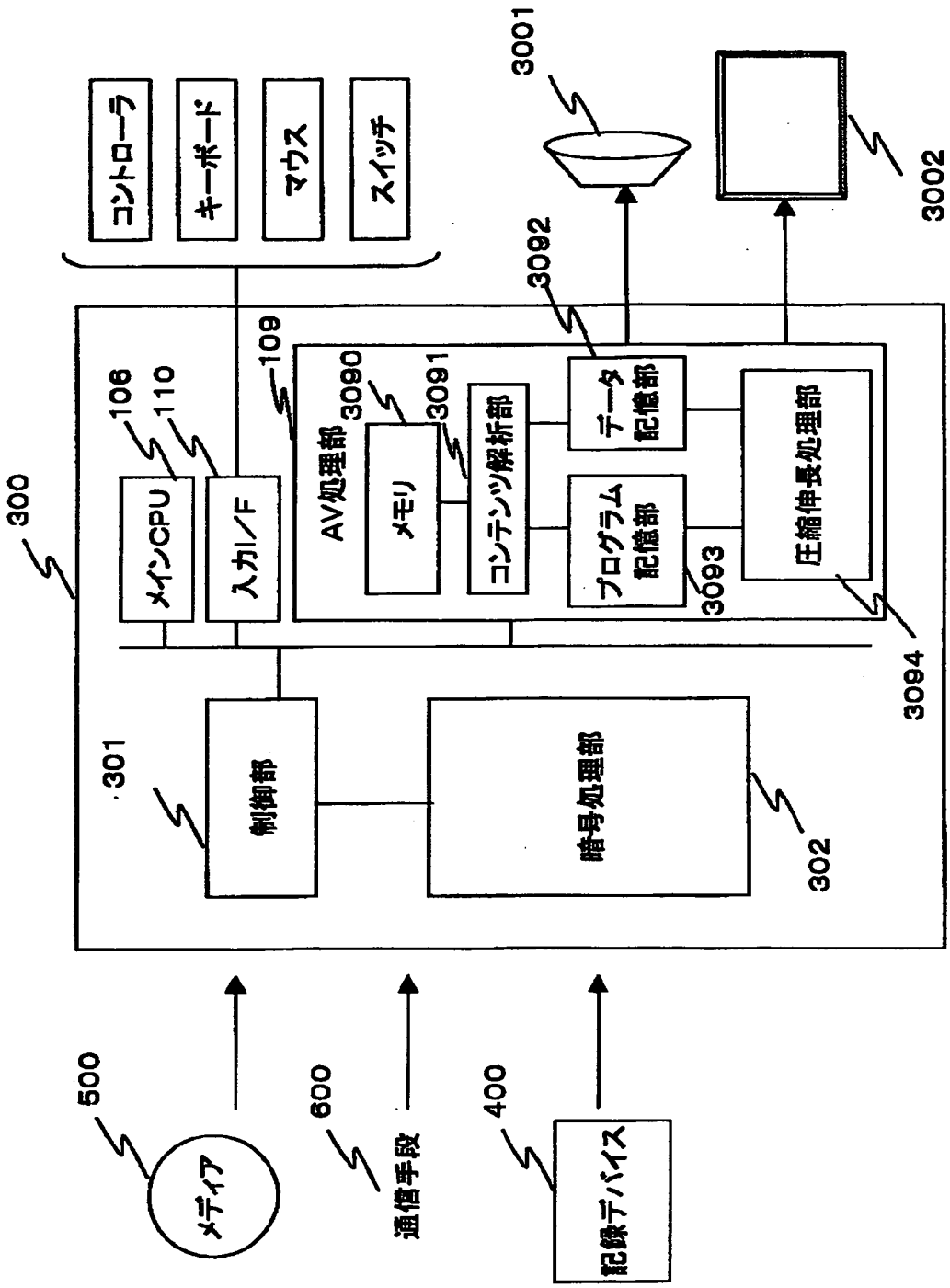
【図５８】


スタート
S621
装着記録デバイス(i)の認証処理
(図20参照)を実行する。
S622
認証成功？
No
Yes
S623
認証済み記録デバイス(i)の記録媒体
から起動可能プログラム
(コンテンツ種類がプログラム)検索
S624
認証済み記録デバイス(i)の記録媒体
中に起動可能プログラム
(コンテンツ種類がプログラム)あり？
No
S627
装着記録デバイスの
コンテンツ検索終了？
No
S628
I=i+1
Yes
S625
起動優先順位の最も高い
プログラムを選択
Yes
S626
選択プログラムを起動
エンド

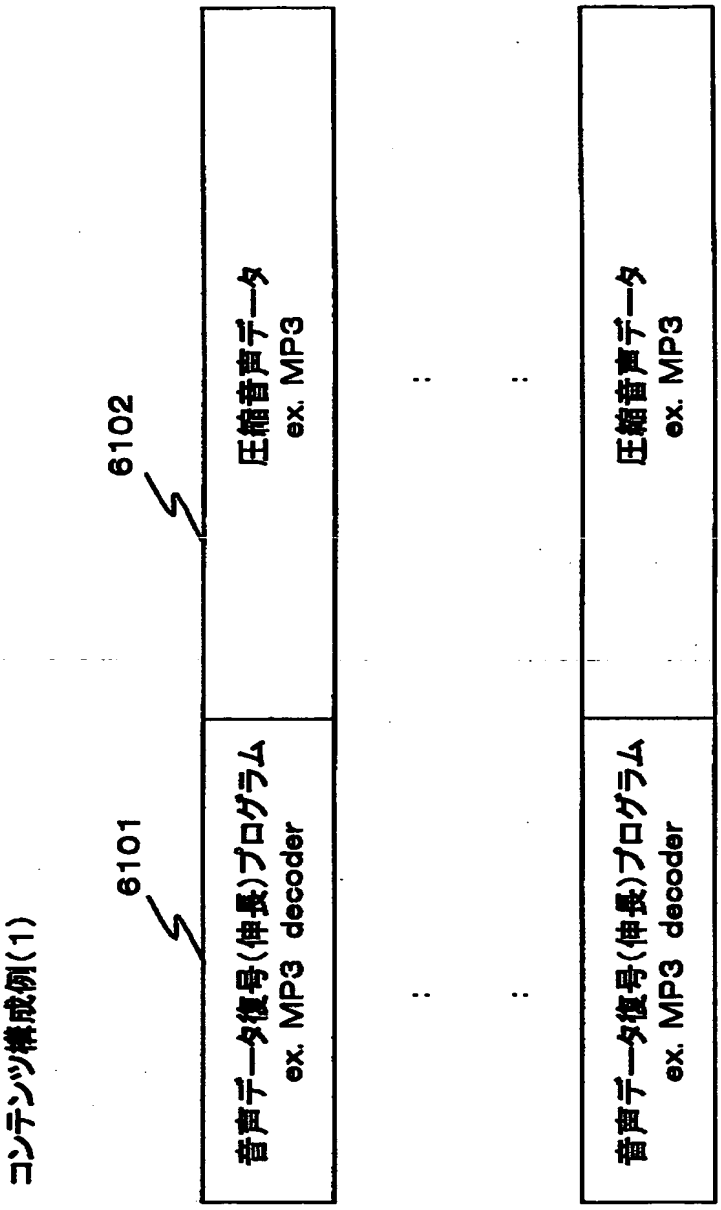
【図５９】


スタート
S651
装着記録デバイスの各々の認証処理
（図20参照）を実行する。
S652
認証済み記録デバイスの記録媒体
から、起動可能プログラム
（コンテンツ種類がプログラム）を抽出
S653
抽出した起動可能プログラム
の情報を表示手段に表示。
S654
ユーザからの起動プログラム
選択入力受信
S655
ユーザ選択プログラム
を起動
エンド

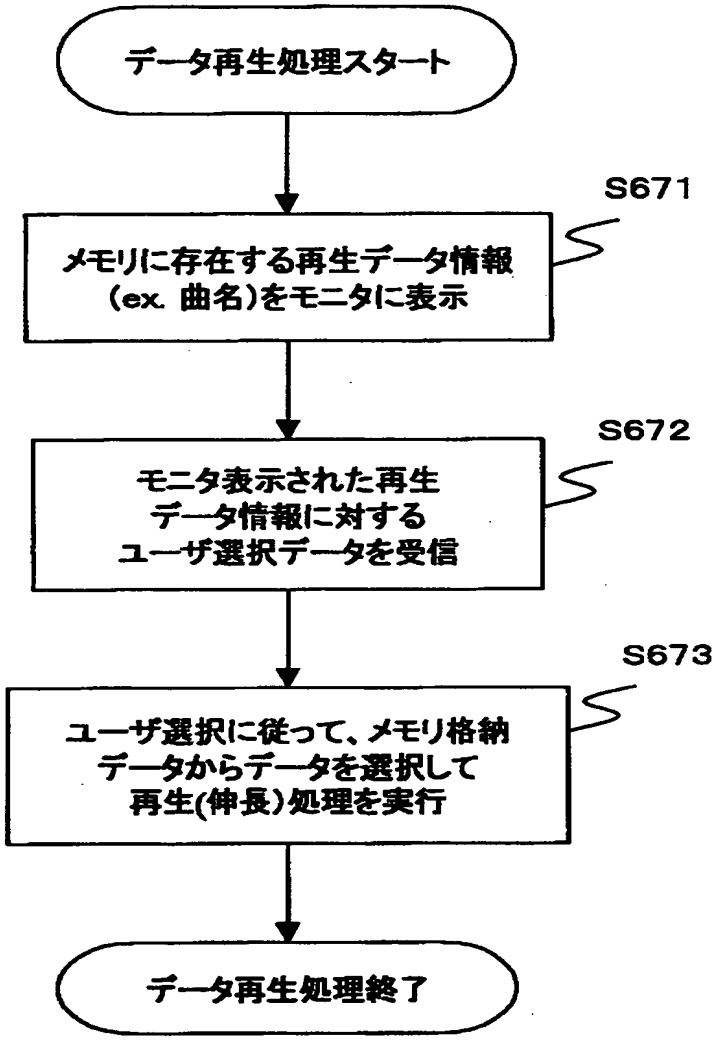
【図６０】


コントローラ
キーボード
マウス
スイッチ
3001
3002
3092
300
106
110
109
3090
3091
メインCPU
入力I/F
AV処理部
メモリ
コンテンツ解析部
データ記憶部
プログラム記憶部
3093
圧縮伸長処理部
3094
301
制御部
暗号処理部
302
500
メディア
600
通信手段
400
記録デバイス

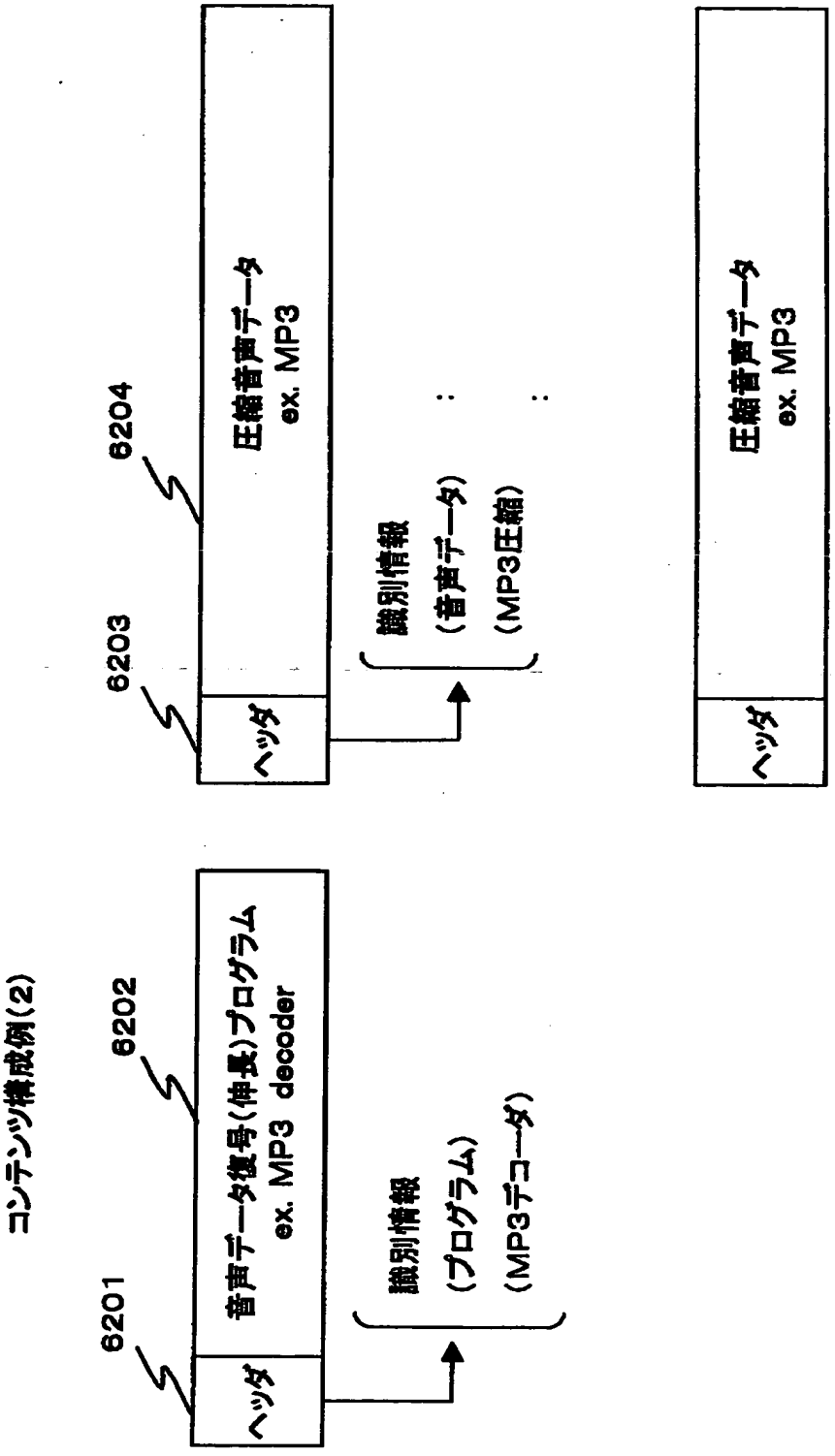
【図６１】


コンテンツ構成例(1)
6101
音声データ復号(伸長)プログラム
ex. MP3 decoder
6102
圧縮音声データ
ex. MP3
音声データ復号(伸長)プログラム
ex. MP3 decoder
圧縮音声データ
ex. MP3

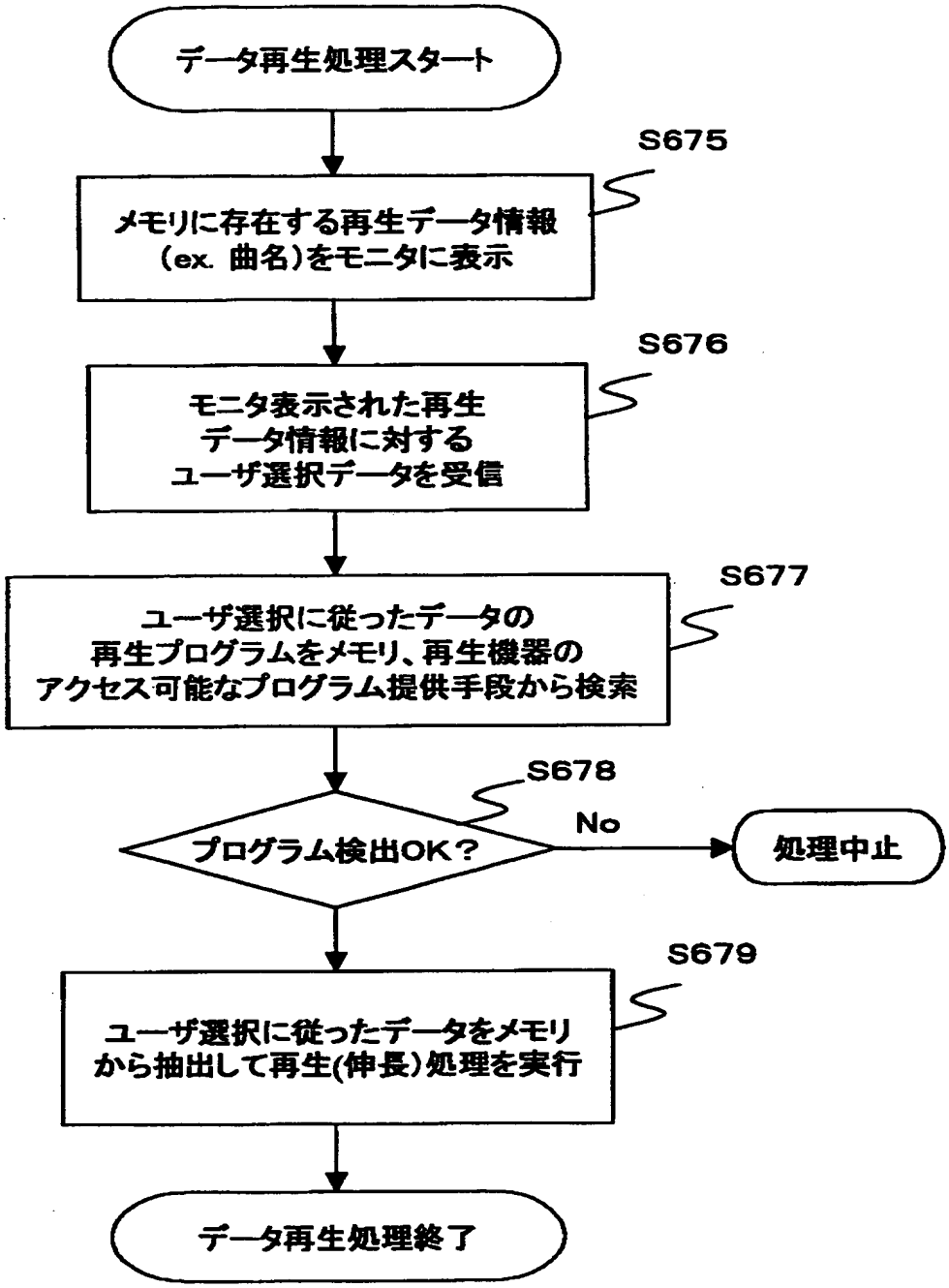
【図６２】


データ再生処理スタート
S671
メモリに存在する再生データ情報
(ex. 曲名)をモニタに表示
S672
モニタ表示された再生
データ情報に対する
ユーザ選択データを受信
S673
ユーザ選択に従って、メモリ格納
データからデータを選択して
再生(伸長)処理を実行
データ再生処理終了

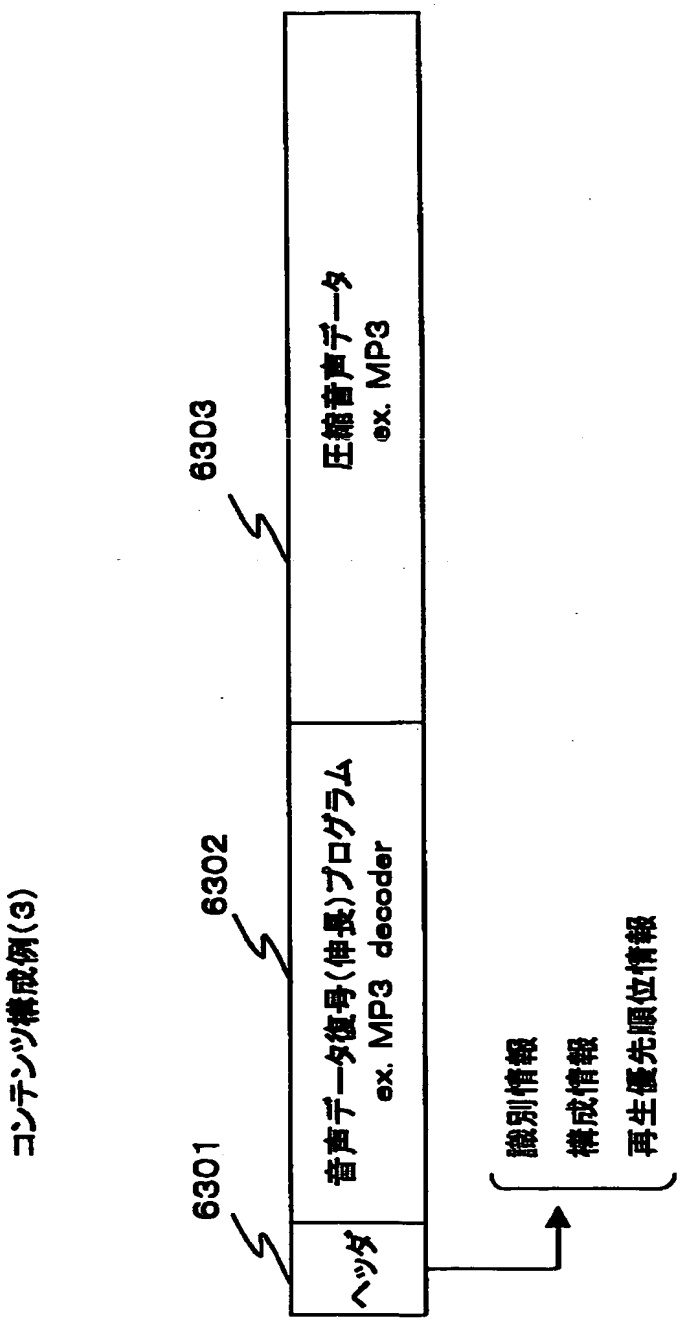
【図６３】


コンテンツ構成例(2)
6201
ヘッダ
6202
音声データ復号(伸長)プログラム
ex. MP3 decoder
識別情報
(プログラム)
(MP3デコーダ)
6203
ヘッダ
6204
圧縮音声データ
ex. MP3
識別情報
(音声データ)
(MP3圧縮)
ヘッダ
圧縮音声データ
ex. MP3

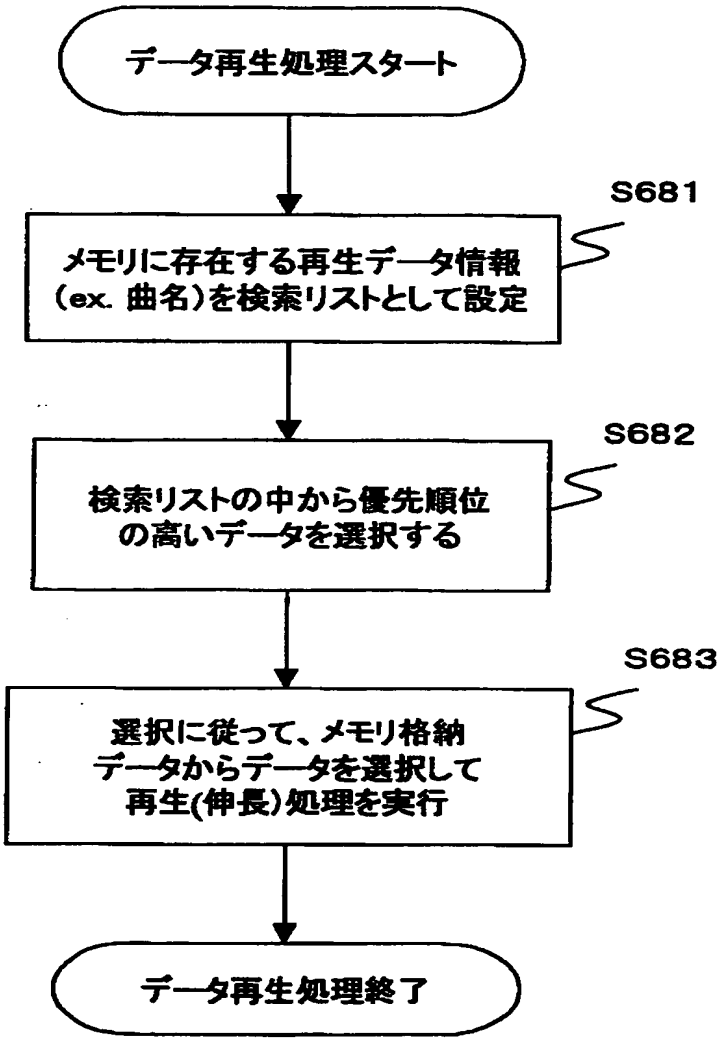
【図６４】


データ再生処理スタート
S675
メモリに存在する再生データ情報
(ex. 曲名)をモニタに表示
S676
モニタ表示された再生
データ情報に対する
ユーザ選択データを受信
S677
ユーザ選択に従ったデータの
再生プログラムをメモリ、再生機器の
アクセス可能なプログラム提供手段から検索
S678
プログラム検出OK？
No
処理中止
S679
ユーザ選択に従ったデータをメモリ
から抽出して再生(伸長)処理を実行
データ再生処理終了

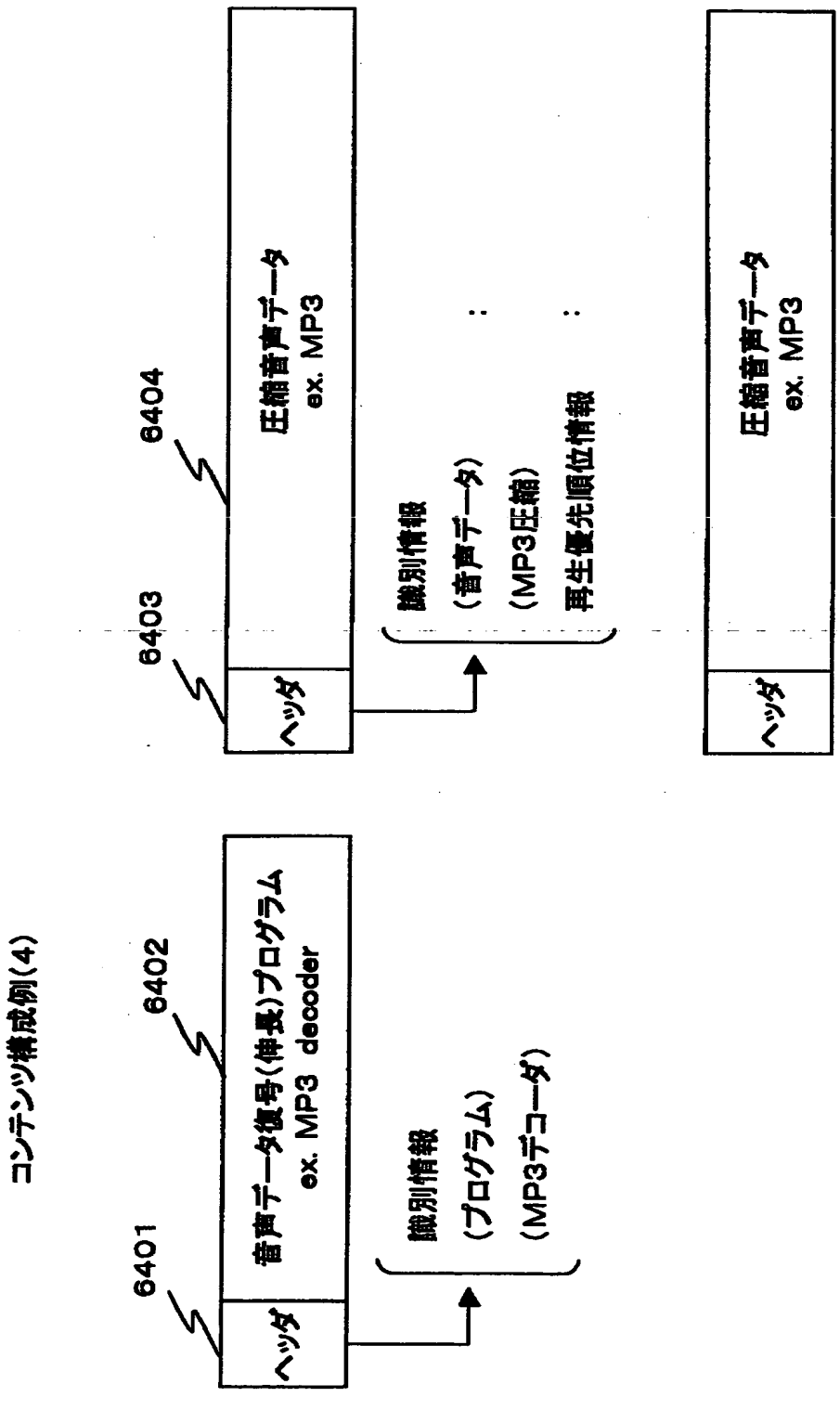
【図６５】


コンテンツ構成例(3)
6301
ヘッダ
6302
音声データ復号(伸長)プログラム
ex. MP3 decoder
6303
圧縮音声データ
ex. MP3
識別情報
構成情報
再生優先順位情報

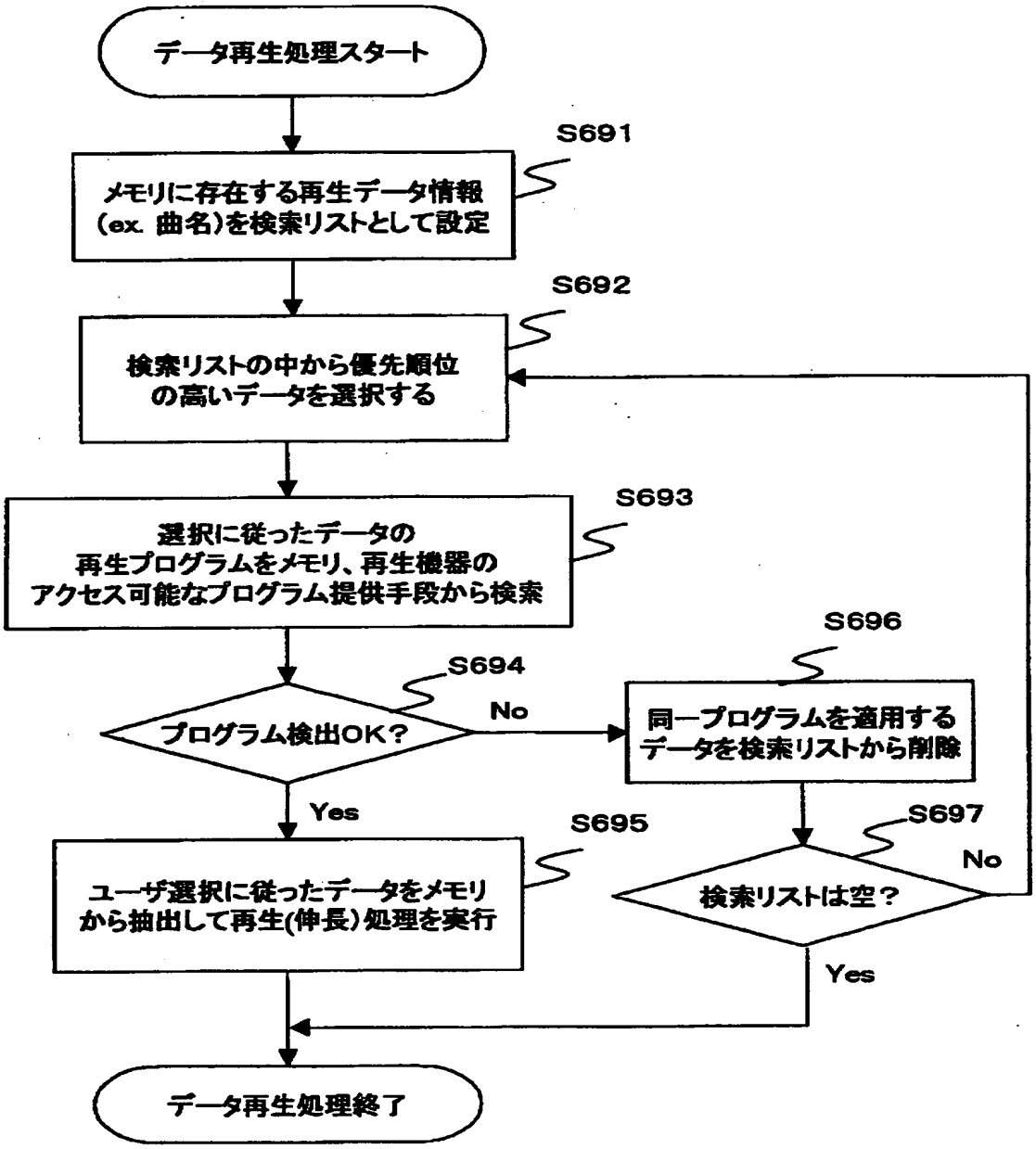
【図６６】


データ再生処理スタート
S681
メモリに存在する再生データ情報
(ex. 曲名)を検索リストとして設定
S682
検索リストの中から優先順位
の高いデータを選択する
S683
選択に従って、メモリ格納
データからデータを選択して
再生(伸長)処理を実行
データ再生処理終了

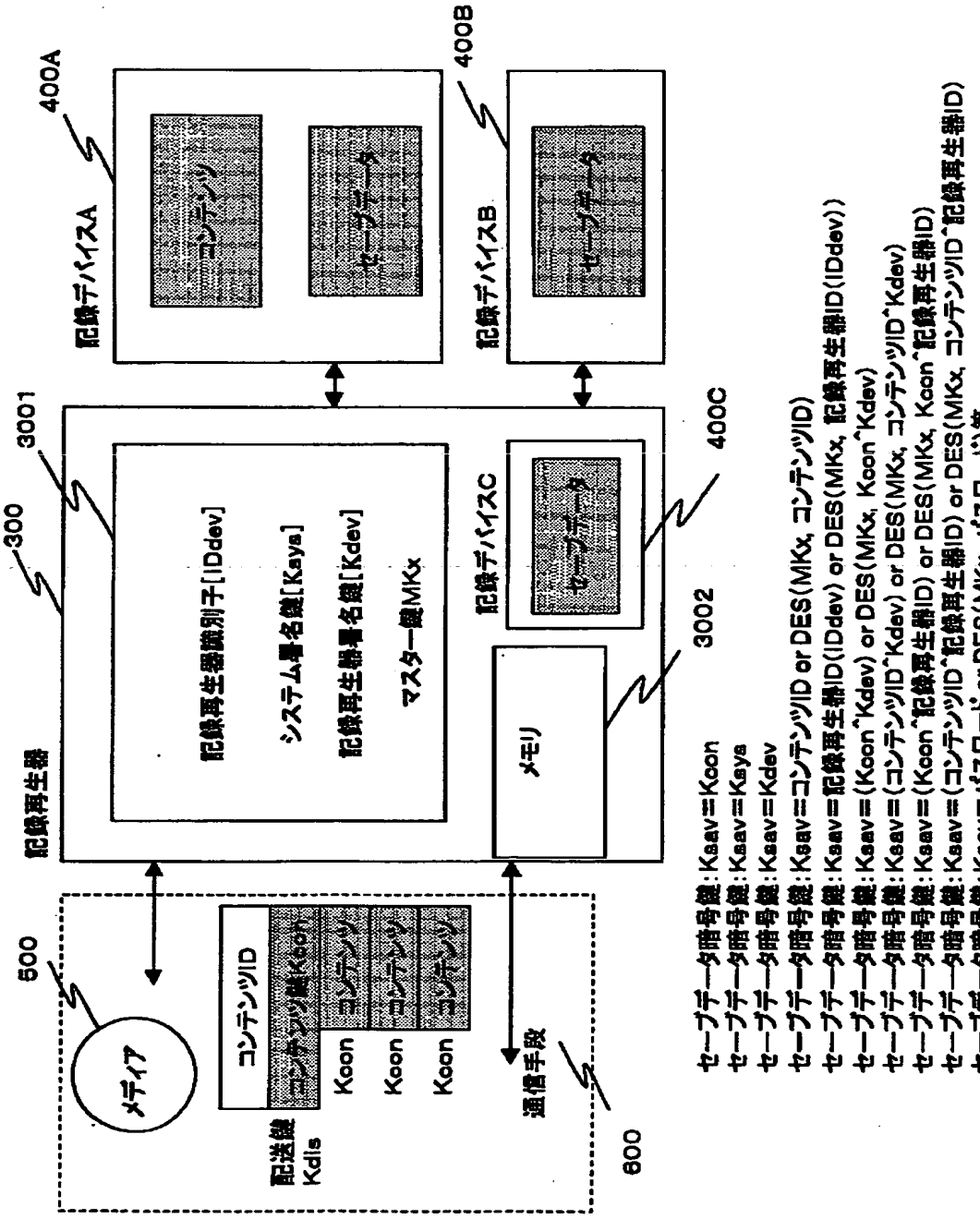
【図６７】


コンテンツ構成例(4)
6401
ヘッダ
6402
音声データ復号(伸長)プログラム
ex. MP3 decoder
識別情報
(プログラム)
(MP3デコーダ)
6403
ヘッダ
6404
圧縮音声データ
ex. MP3
識別情報
(音声データ)
(MP3圧縮)
再生優先順位情報
ヘッダ
圧縮音声データ
ex. MP3

【図６８】

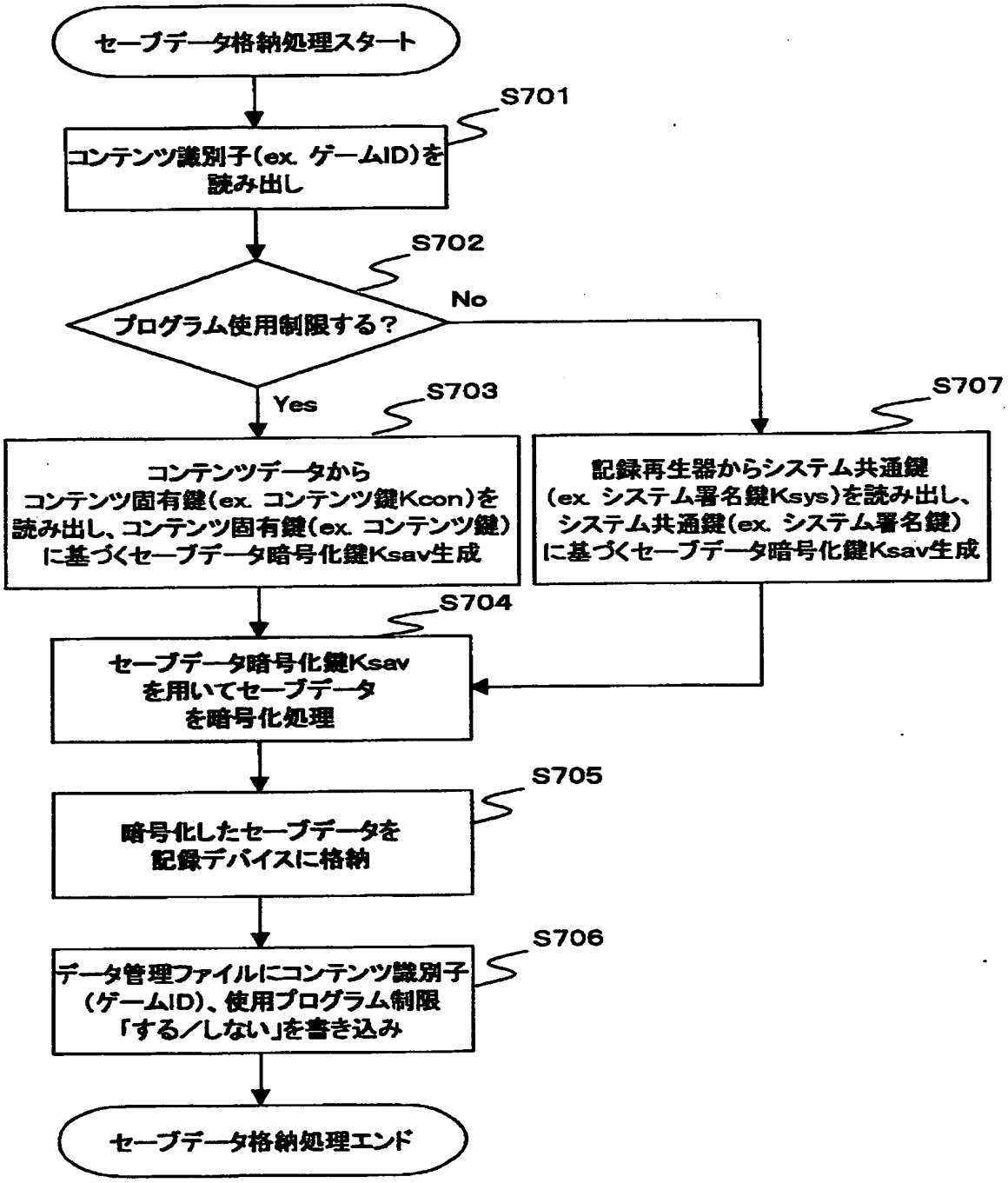

データ再生処理スタート
S691
メモリに存在する再生データ情報
(ex. 曲名)を検索リストとして設定
S692
検索リストの中から優先順位
の高いデータを選択する
S693
選択に従ったデータの
再生プログラムをメモリ、再生機器の
アクセス可能なプログラム提供手段から検索
S694
プログラム検出OK？
No
S696
同一プログラムを適用する
データを検索リストから削除
Yes
S695
ユーザ選択に従ったデータをメモリ
から抽出して再生(伸長)処理を実行
S697
検索リストは空？
No
Yes
データ再生処理終了

【図６９】


400A
400B
記録デバイスA
記録デバイスB
コンテンツ
セーブデータ
セーブデータ
3001
300
400C
記録再生器
記録再生器識別子[IDdev]
システム暑名鍵[Kaya]
記録再生器暑名鍵[Kdev]
マスター鍵MKx
記録デバイスC
セーブデータ
メモリ
3002
500
メディア
コンテンツID
コンテンツ鍵Kcon
コンテンツ
コンテンツ
コンテンツ
Kcon
Kcon
Kcon
配送鍵
Kdis
通信手段
600
セーブデータ暗号鍵:Kaav=Kcon
セーブデータ暗号鍵:Kaav=Kaya
セーブデータ暗号鍵:Kaav=Kdev
セーブデータ暗号鍵:Kaav=コンテンツID or DES(MKx, コンテンツID)
セーブデータ暗号鍵:Kaav=記録再生器ID(IDdev) or DES(MKx, 記録再生器ID(IDdev))
セーブデータ暗号鍵:Kaav=(Kcon^Kdev) or DES(MKx, Kcon^Kdev)
セーブデータ暗号鍵:Kaav=(コンテンツID^Kdev) or DES(MKx, コンテンツID^Kdev)
セーブデータ暗号鍵:Kaav=(Kcon^記録再生器ID) or DES(MKx, Kcon^記録再生器ID)
セーブデータ暗号鍵:Kaav=(コンテンツID^記録再生器ID) or DES(MKx, コンテンツID^記録再生器ID)
セーブデータ暗号鍵:Kaav=パスワード or DES(MKx, パスワード)等

【図７０】

(1)コンテンツ固有鍵、orシステム共通鍵を使用したセーブデータ格納処理例



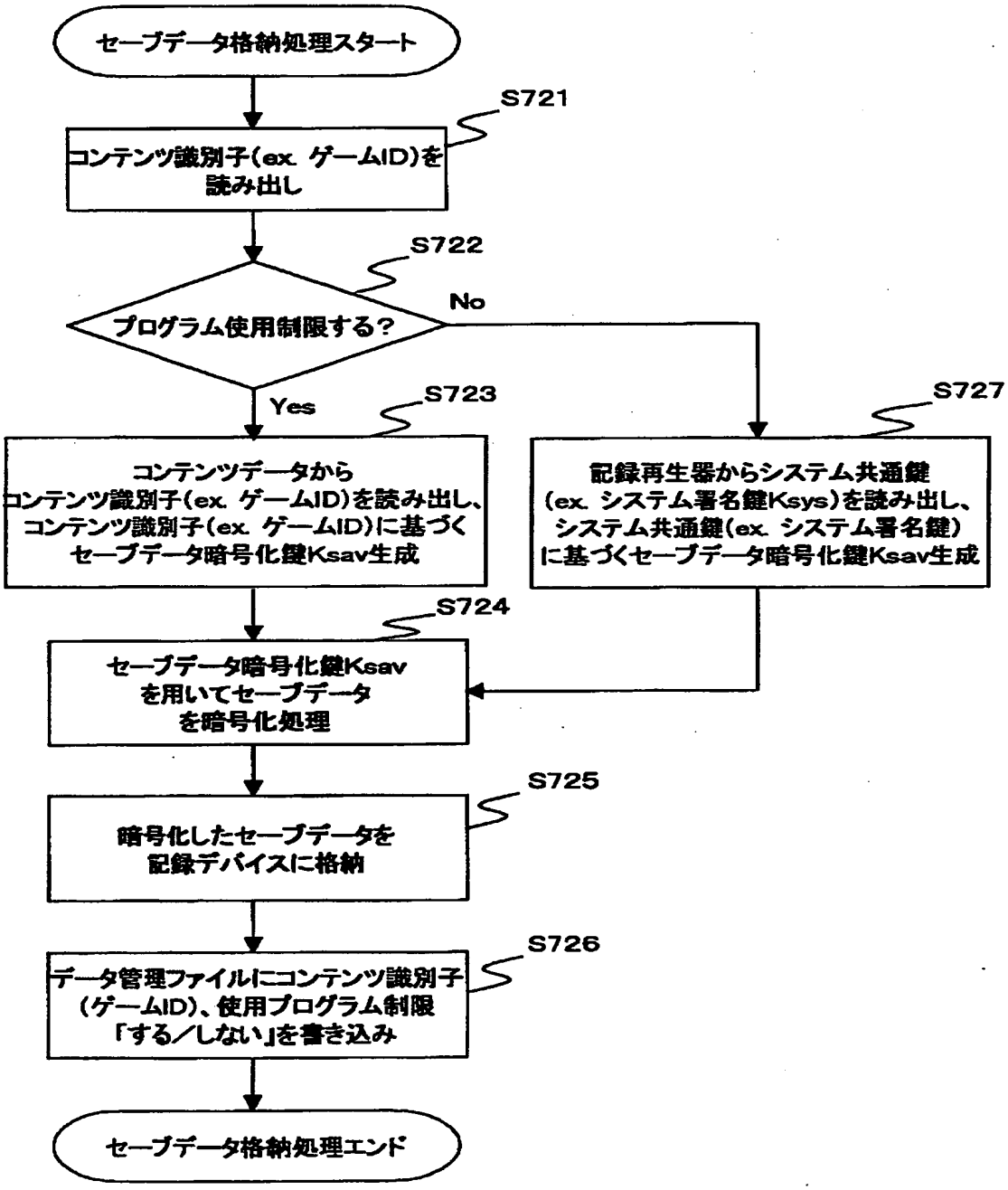
【図７１】

データ管理ファイル(1)

データ番号	コンテンツ識別子 (ゲームID)	記録再生装置識別子 (IDdev)	プログラム使用制限
1	12345678...	56789012...	する
2	ABCDEF12...	09876543...	する
3	12245767 8...	58834762...	しない
:	:	:	:

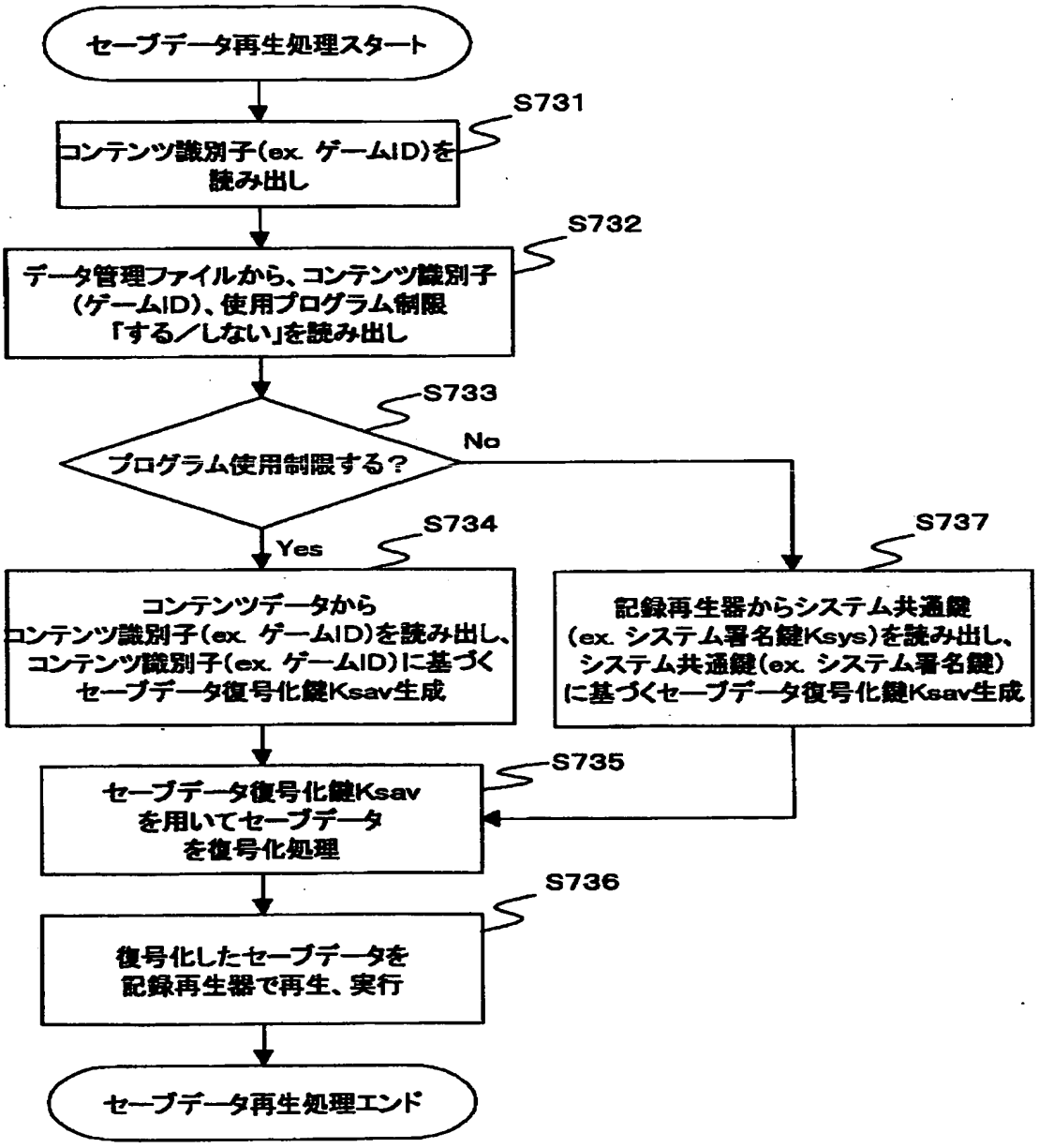
【図７３】

(3)コンテンツID、orシステム共通鍵を使用したセーブデータ格納処理例



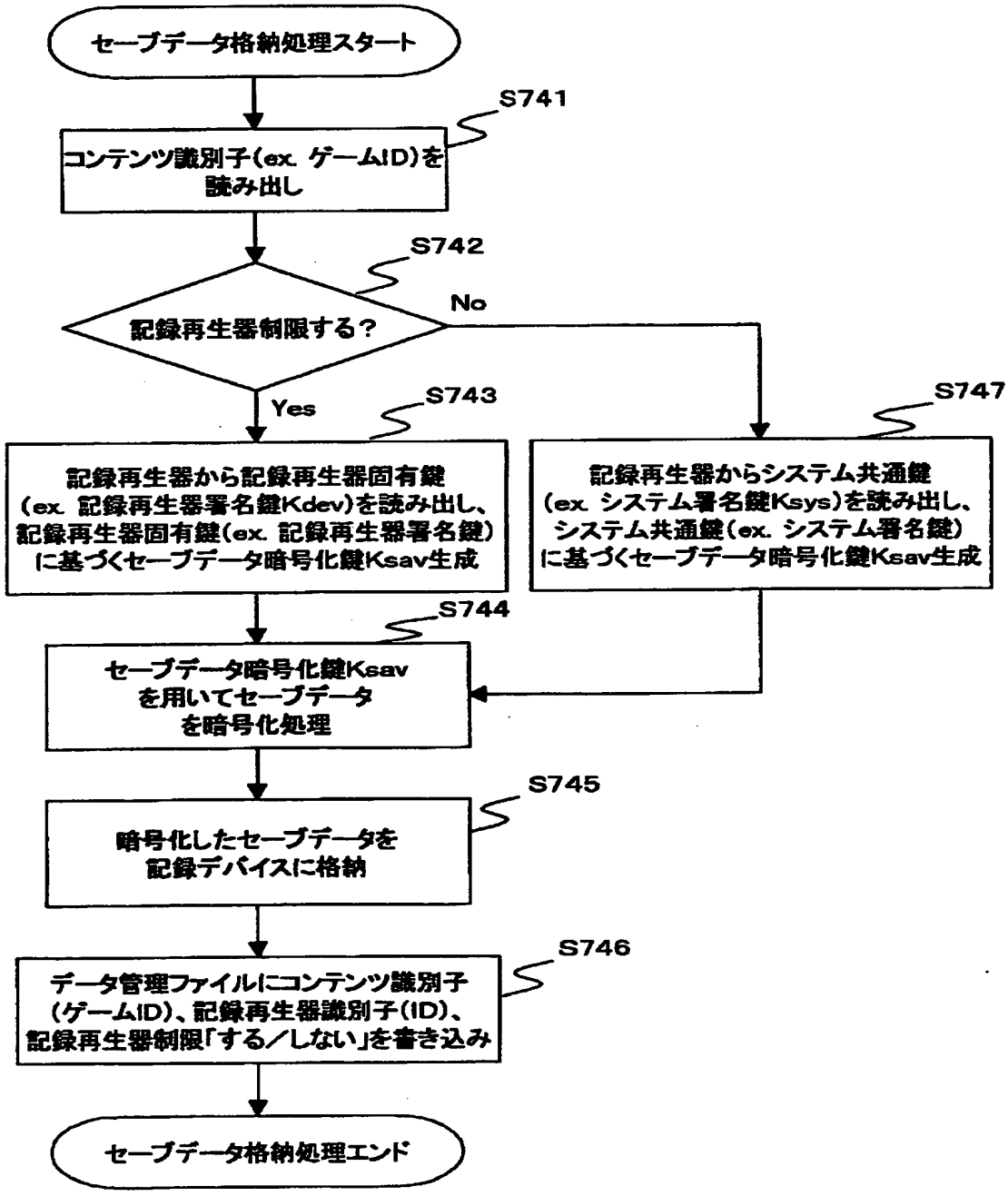
【図７４】

(4)コンテンツID、orシステム共通鍵を使用したセーブデータ再生処理例

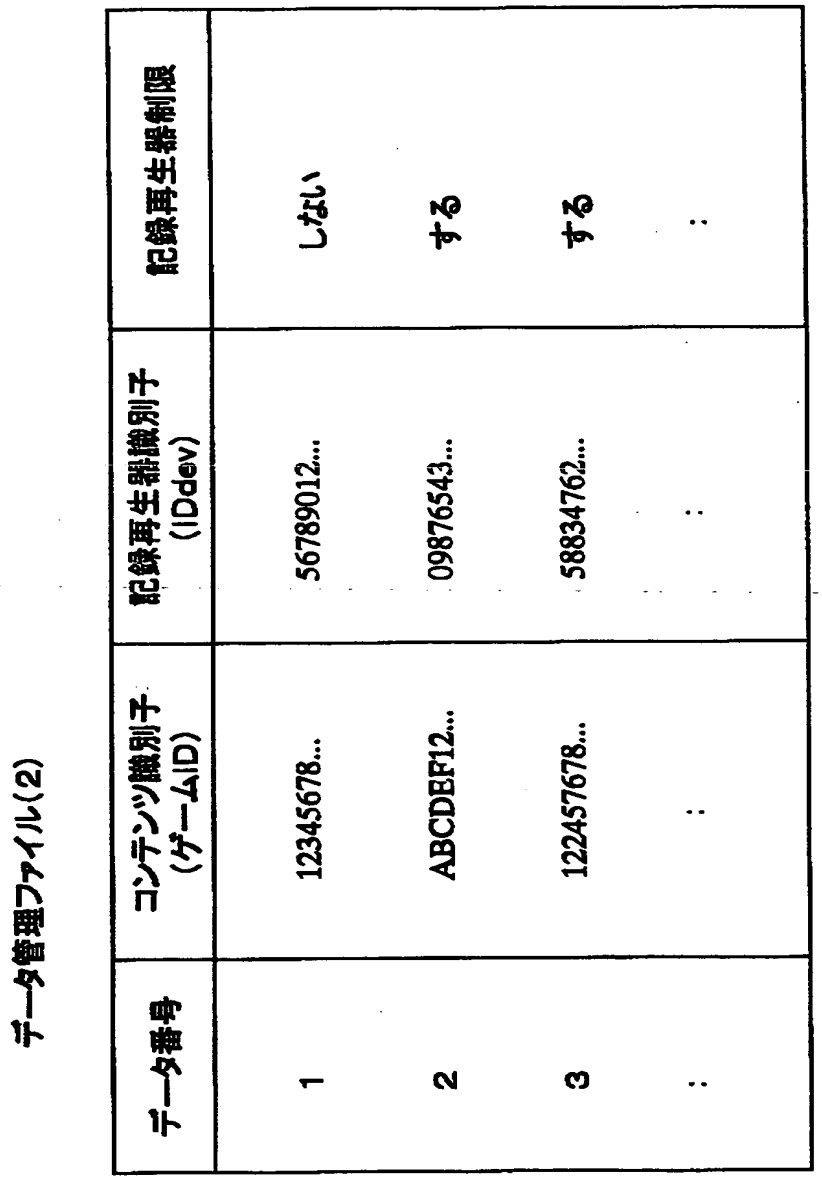


【図７５】

(5)記録再生器固有鍵、or システム共通鍵を使用したセーブデータ格納処理例



【図７６】

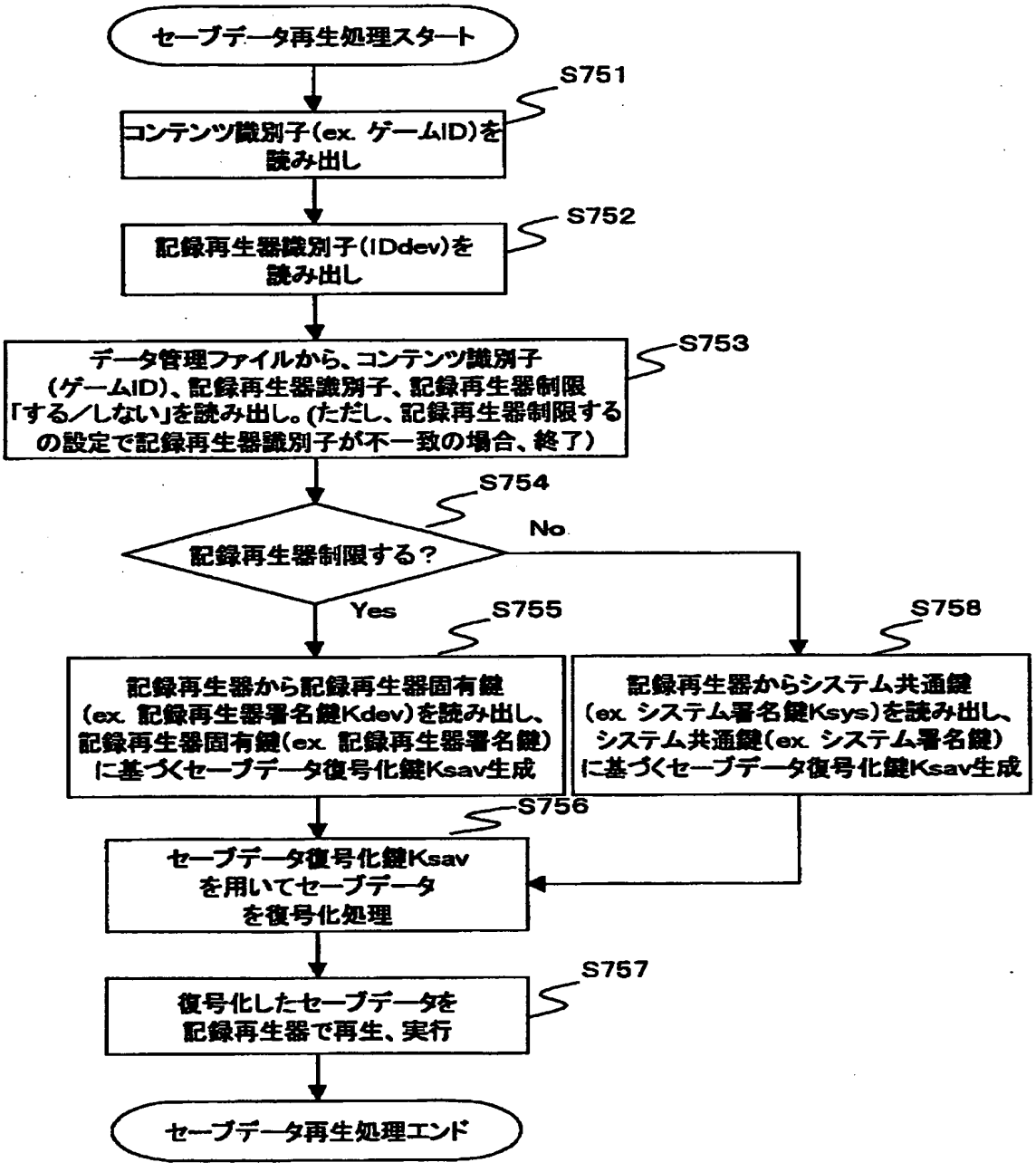


データ管理ファイル(2)

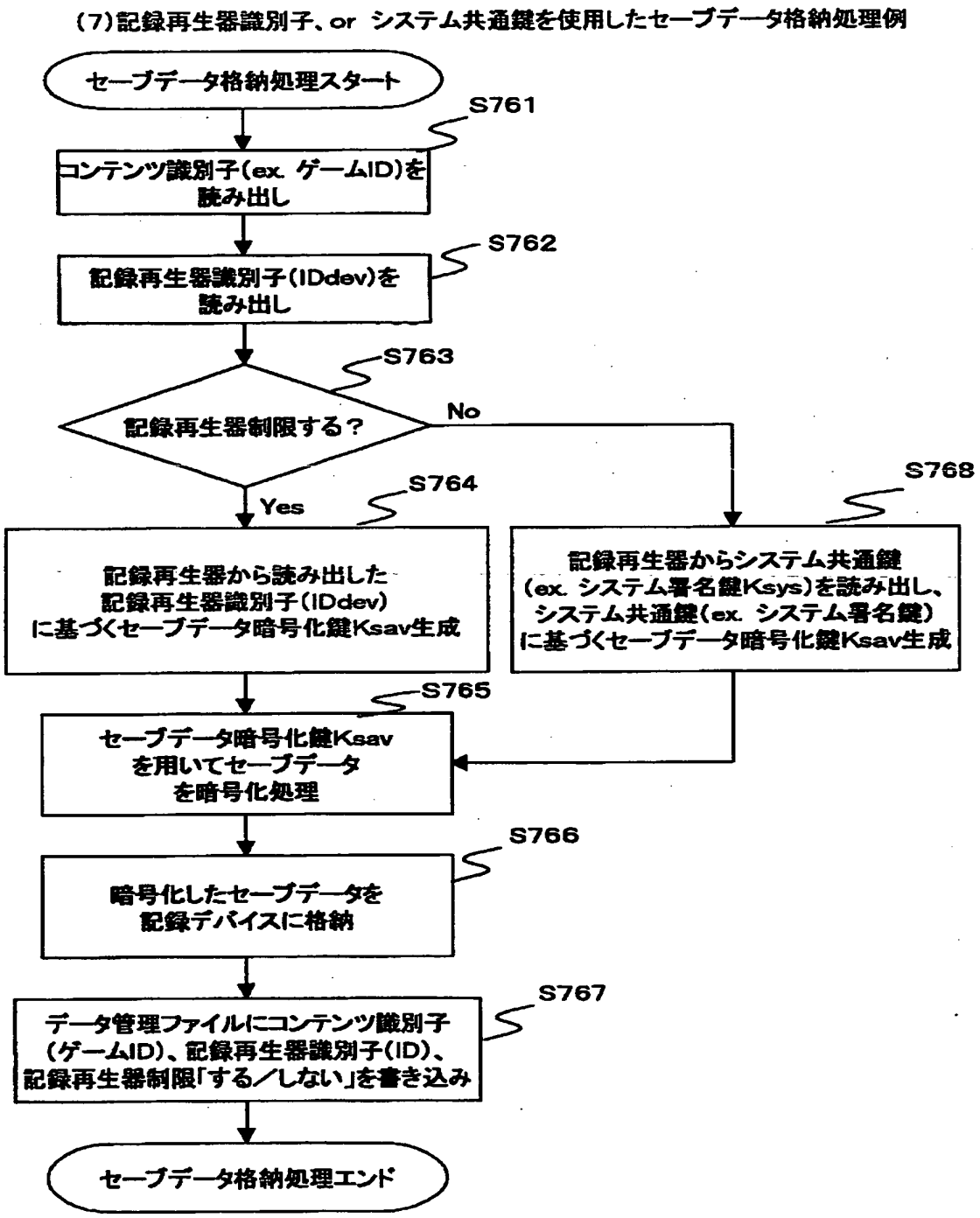
データ番号	コンテンツ識別子（ゲームID）	記録再生器識別子（IDdev）	記録再生器制限
1	12345678...	56789012...	しない
2	ABCDEF12...	09876543...	する
3	12245767 8...	58834762...	する
：	：	：	：

【図７７】

(6)記録再生器固有鍵、or システム共通鍵を使用したセーブデータ再生処理例

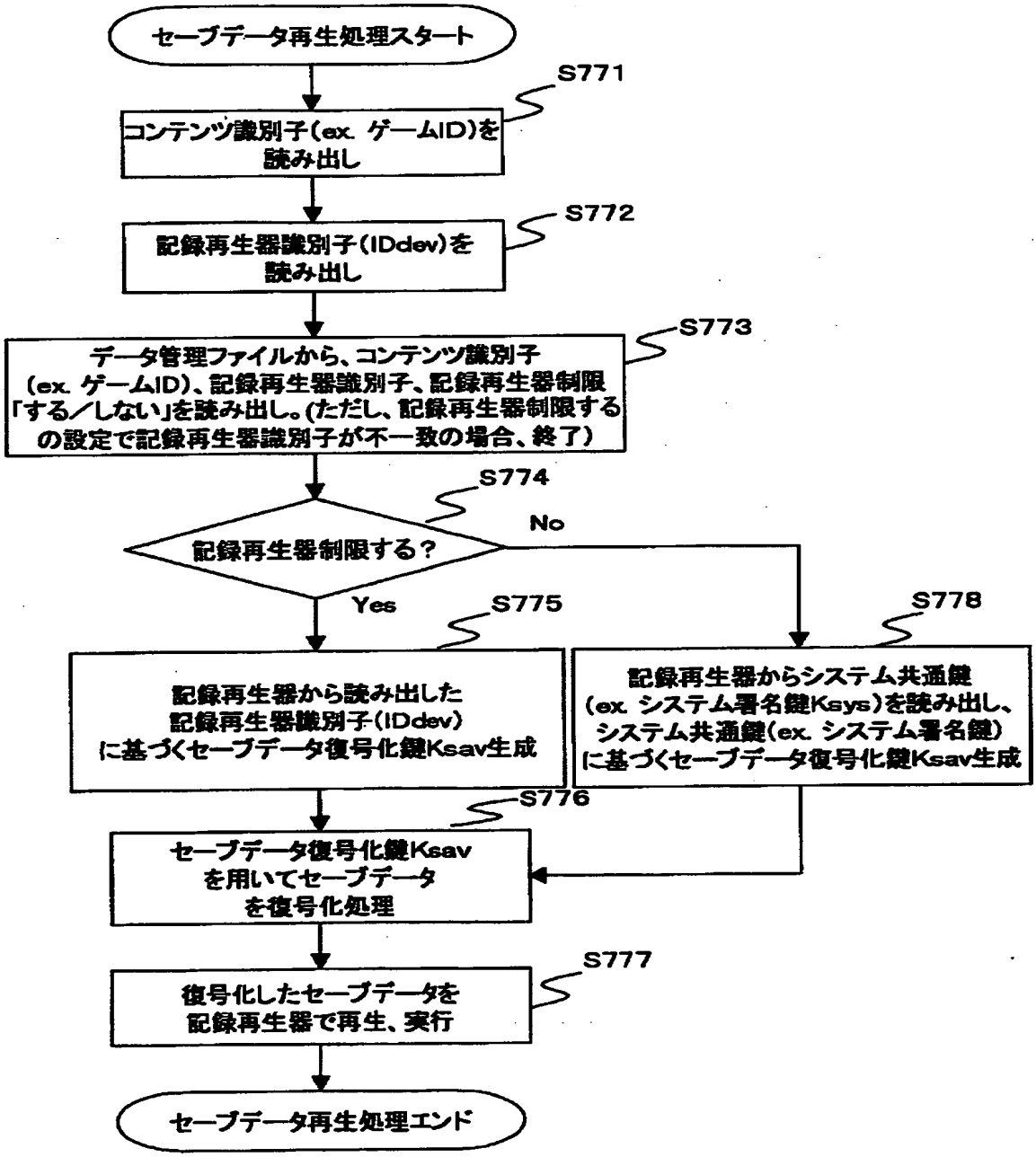


【図７８】

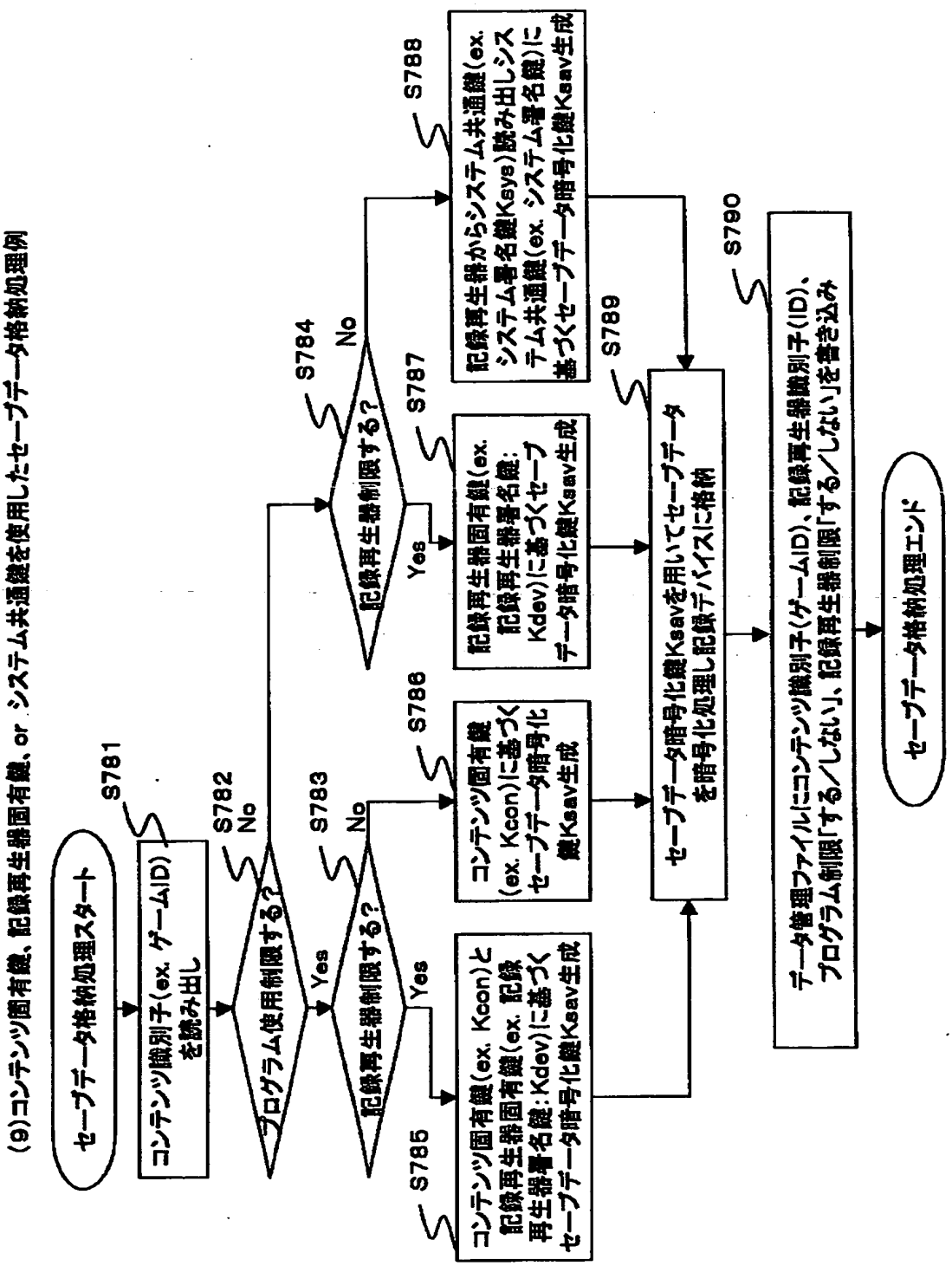

(7)記録再生器識別子、or システム共通鍵を使用したセーブデータ格納処理例
セーブデータ格納処理スタート
S761
コンテンツ識別子(ex. ゲームID)を読み出し
S762
記録再生器識別子(IDdev)を読み出し
S763
記録再生器制限する？
No
Yes
S764
記録再生器から読み出した記録再生器識別子(IDdev)に基づくセーブデータ暗号化鍵Ksav生成
S768
記録再生器からシステム共通鍵(ex. システム署名鍵Ksys)を読み出し、システム共通鍵(ex. システム署名鍵)に基づくセーブデータ暗号化鍵Ksav生成
S765
セーブデータ暗号化鍵Ksavを用いてセーブデータを暗号化処理
S766
暗号化したセーブデータを記録デバイスに格納
S767
データ管理ファイルにコンテンツ識別子(ゲームID)、記録再生器識別子(ID)、記録再生器制限「する／しない」を書き込み
セーブデータ格納処理エンド

【図７９】

(8)記録再生器識別子、or システム共通鍵を使用したセーブデータ再生処理例



【図８０】

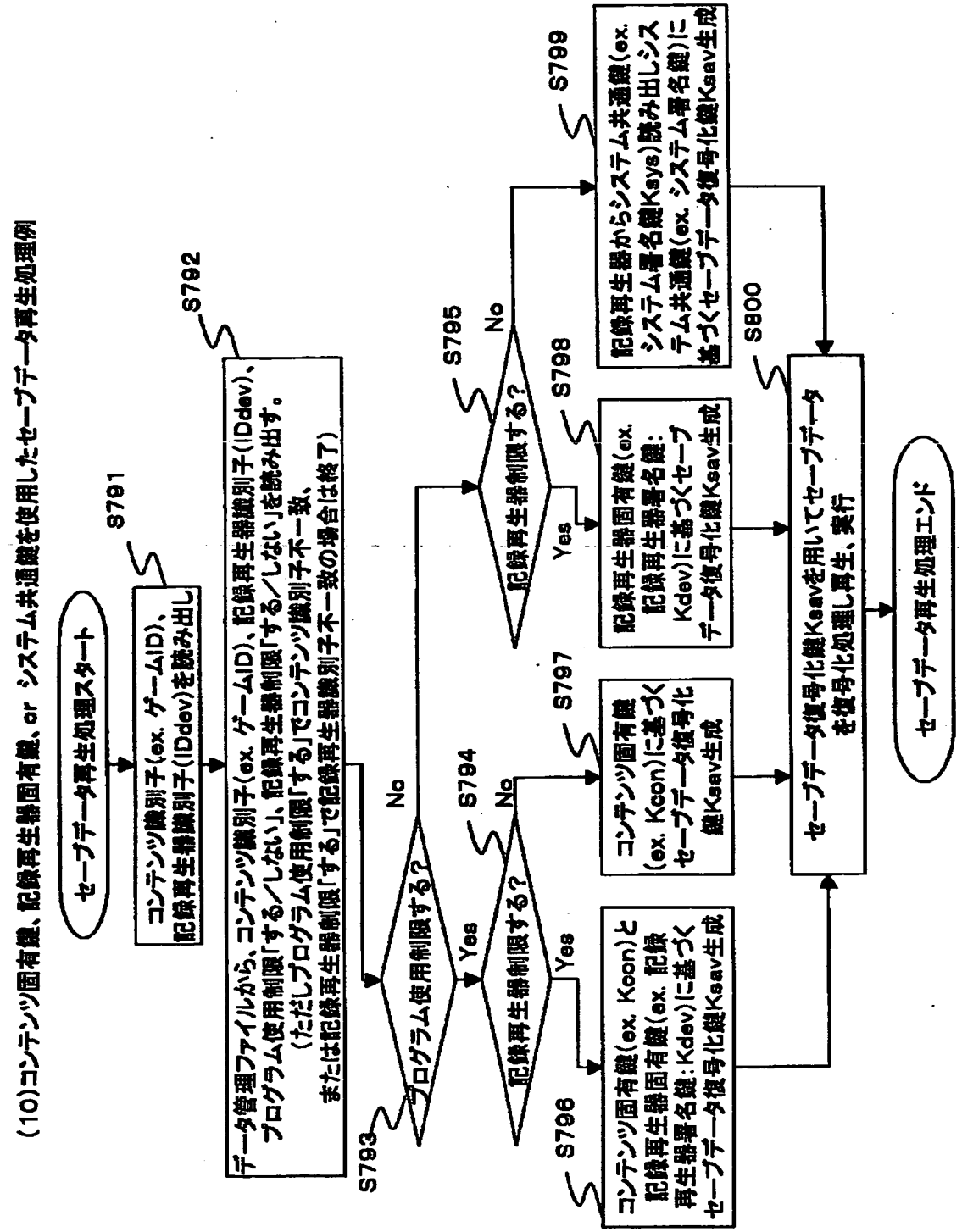

(9)コンテンツ固有鍵、記録再生器固有鍵、or システム共通鍵を使用したセーブデータ格納処理例
セーブデータ格納処理スタート
S781
コンテンツ識別子(ex. ゲームID)を読み出し
S782
No
プログラム使用制限する?
Yes
S783
No
記録再生器制限する?
Yes
S784
No
記録再生器制限する?
Yes
S785
コンテンツ固有鍵(ex. Kcon)と記録再生器固有鍵(ex. 記録再生器署名鍵:Kdev)に基づくセーブデータ暗号化鍵Ksav生成
S786
コンテンツ固有鍵(ex. Kcon)に基づくセーブデータ暗号化鍵Ksav生成
S787
記録再生器固有鍵(ex. 記録再生器署名鍵:Kdev)に基づくセーブデータ暗号化鍵Ksav生成
S788
記録再生器からシステム共通鍵(ex. システム署名鍵Ksys)読み出しシステム共通鍵(ex. システム署名鍵)に基づくセーブデータ暗号化鍵Ksav生成
S789
セーブデータ暗号化鍵Ksavを用いてセーブデータを暗号化処理し記録デバイスに格納
S790
データ管理ファイルにコンテンツ識別子(ゲームID)、記録再生器識別子(ID)、プログラム制限「する/しない」、記録再生器制限「する/しない」を書き込み
セーブデータ格納処理エンド

【図８１】

データ管理ファイル(3)

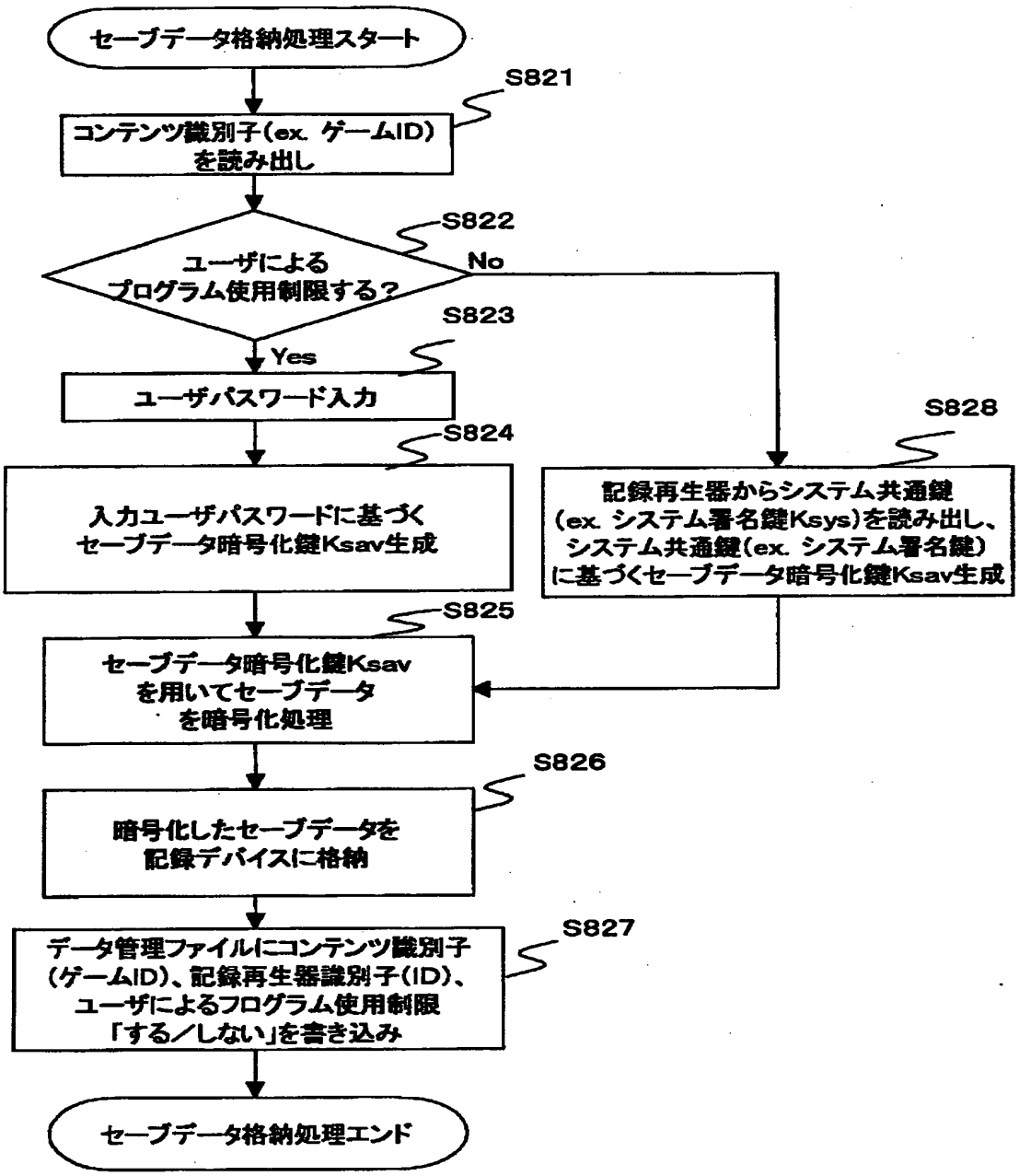
データ番号	コンテンツ識別子 (ゲームID)	記録再生器識別子 (IDdev)	プログラム使用制限	記録再生器制限
1	12345678...	56789012...	する	しない
2	ABCDEF12...	09876543...	する	する
3	122457678...	58834762...	しない	する
⋮	⋮	⋮	⋮	⋮

【図８２】


(10)コンテンツ固有鍵、記録再生器固有鍵、or システム共通鍵を使用したセーブデータ再生処理例
セーブデータ再生処理スタート
S791
コンテンツ識別子(ex. ゲームID)、記録再生器識別子(IDdev)を読み出し
S792
データ管理ファイルから、コンテンツ識別子(ex. ゲームID)、記録再生器識別子(IDdev)、プログラム使用制限「する/しない」、記録再生器制限「する/しない」を読み出す。
(ただしプログラム使用制限「する」でコンテンツ識別子不一致、または記録再生器制限「する」で記録再生器識別子不一致の場合は終了)
S793
プログラム使用制限する?
No
Yes
S794
記録再生器制限する?
No
Yes
S795
記録再生器制限する?
No
Yes
S796
コンテンツ固有鍵(ex. Kcon)と記録再生器固有鍵(ex. 記録再生器署名鍵:Kdev)に基づくセーブデータ復号化鍵Ksav生成
S797
コンテンツ固有鍵(ex. Kcon)に基づくセーブデータ復号化鍵Ksav生成
S798
記録再生器固有鍵(ex. 記録再生器署名鍵:Kdev)に基づくセーブデータ復号化鍵Ksav生成
S799
記録再生器からシステム共通鍵(ex. システム署名鍵Ksys)読み出しシステム共通鍵(ex. システム署名鍵)に基づくセーブデータ復号化鍵Ksav生成
S800
セーブデータ復号化鍵Ksavを用いてセーブデータを復号化処理し再生、実行
セーブデータ再生処理エンド

【図８３】

(11)ユーザパスワード、or システム共通鍵を使用したセーブデータ格納処理例



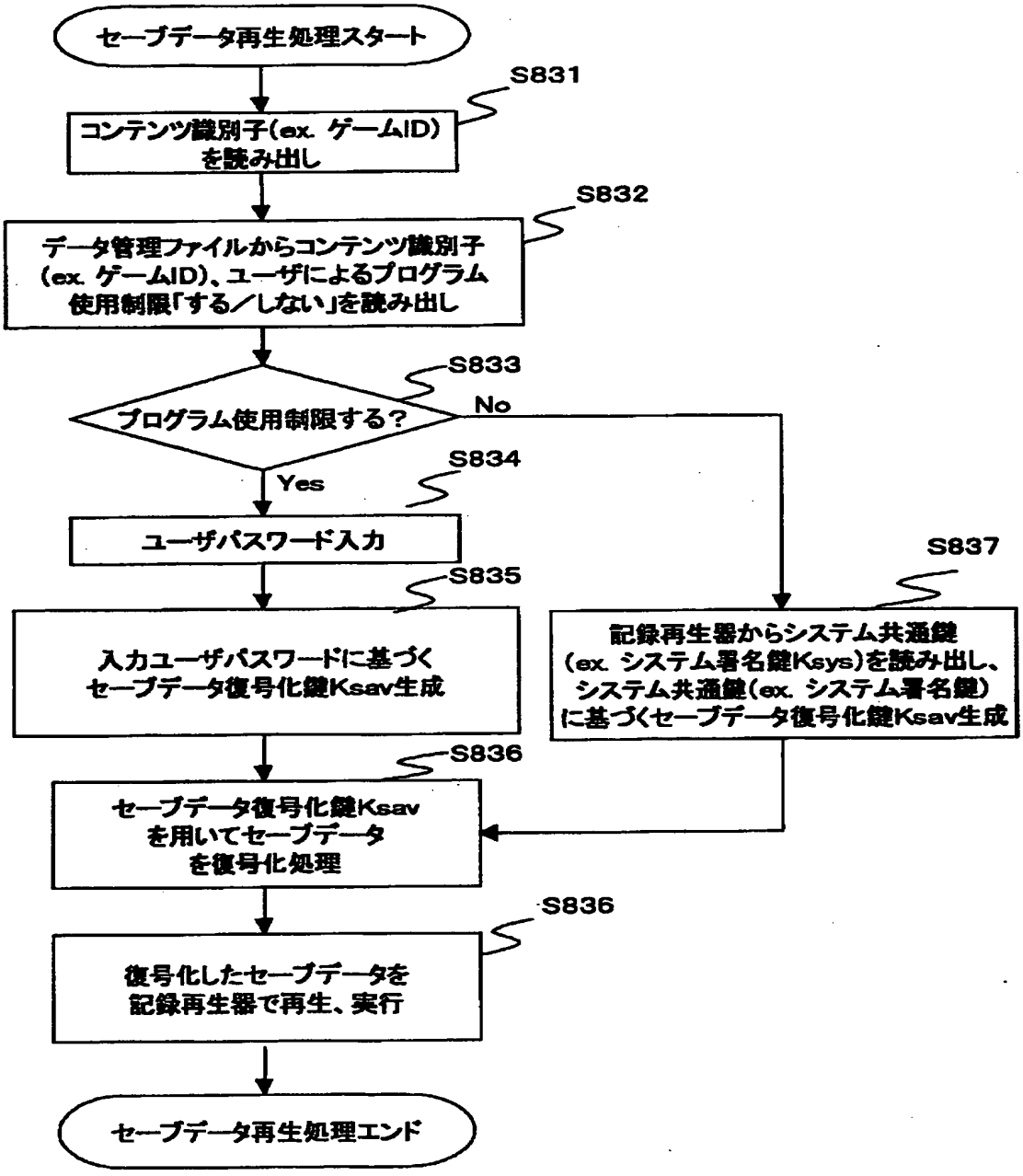
【図８４】

データ管理ファイル(4)

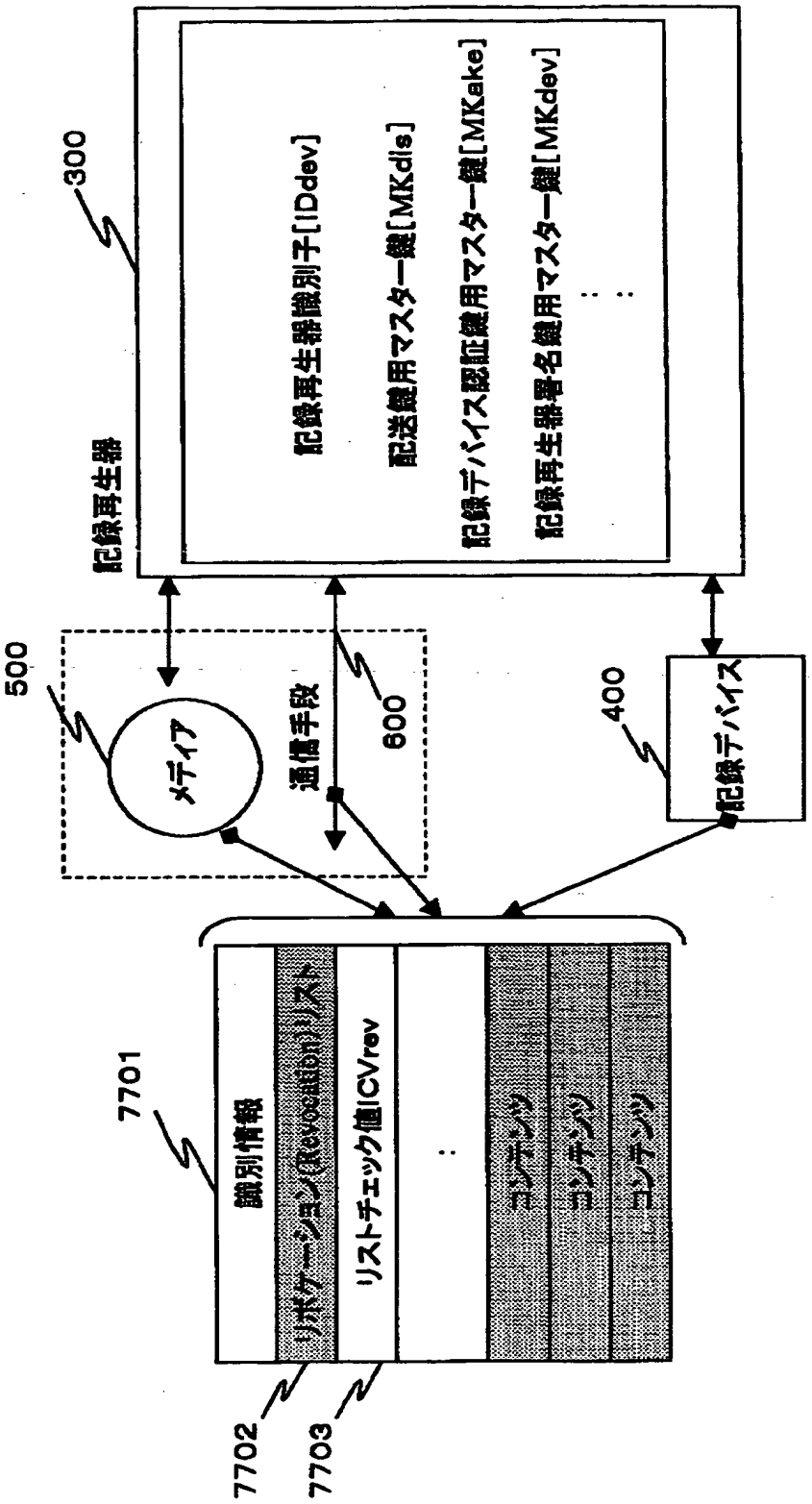
データ番号	コンテンツ識別子（ゲームID）	記録再生機識別子（IDdev）	ユーザによるプログラム使用制限
1	12345678...	56789012...	する
2	ABCDEF12...	09876543...	する
3	122457678...	58834762...	しない
..	..	..	..

【図８５】

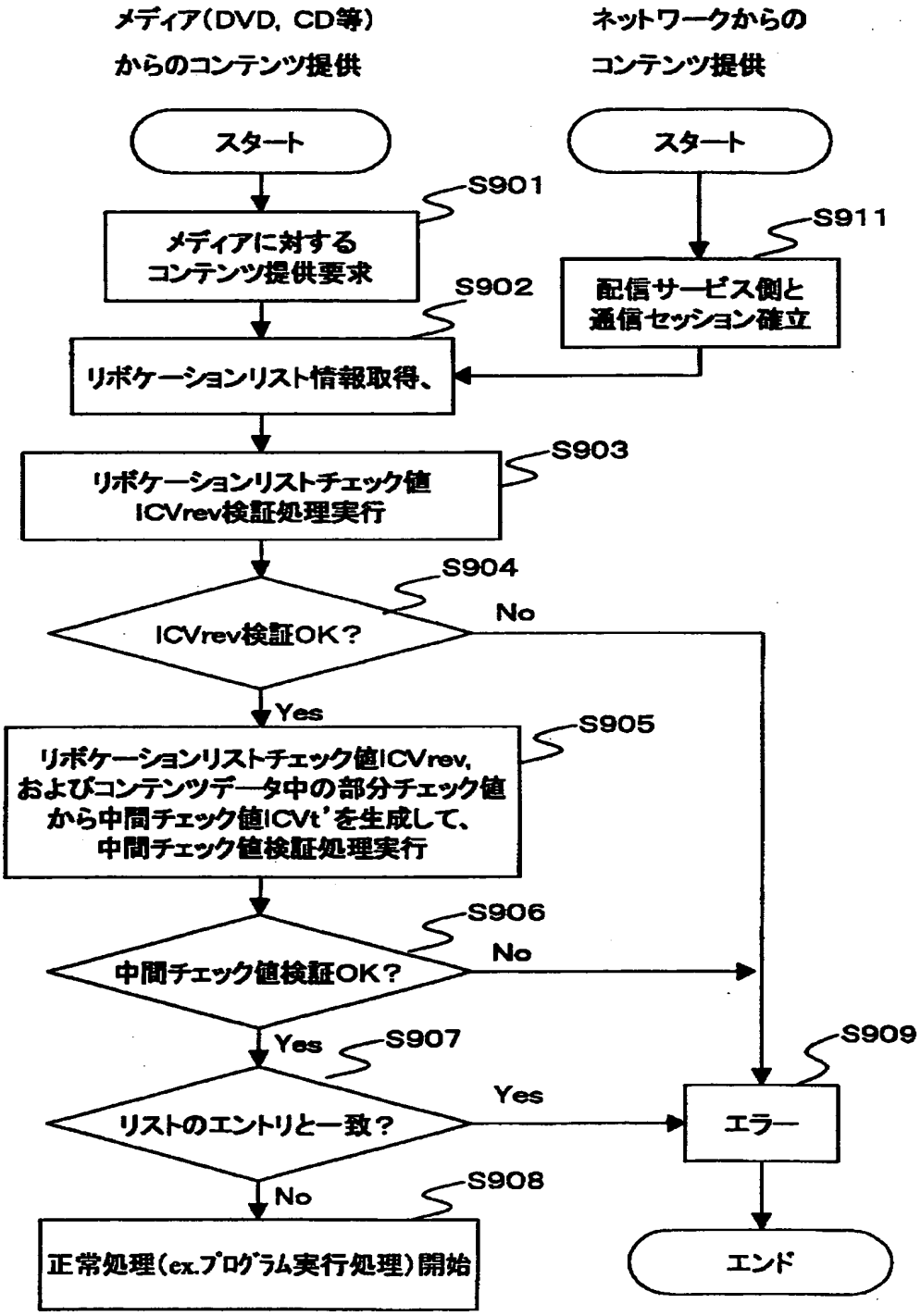
(12)ユーザパスワード、or システム共通鍵を使用したセーブデータ再生処理例



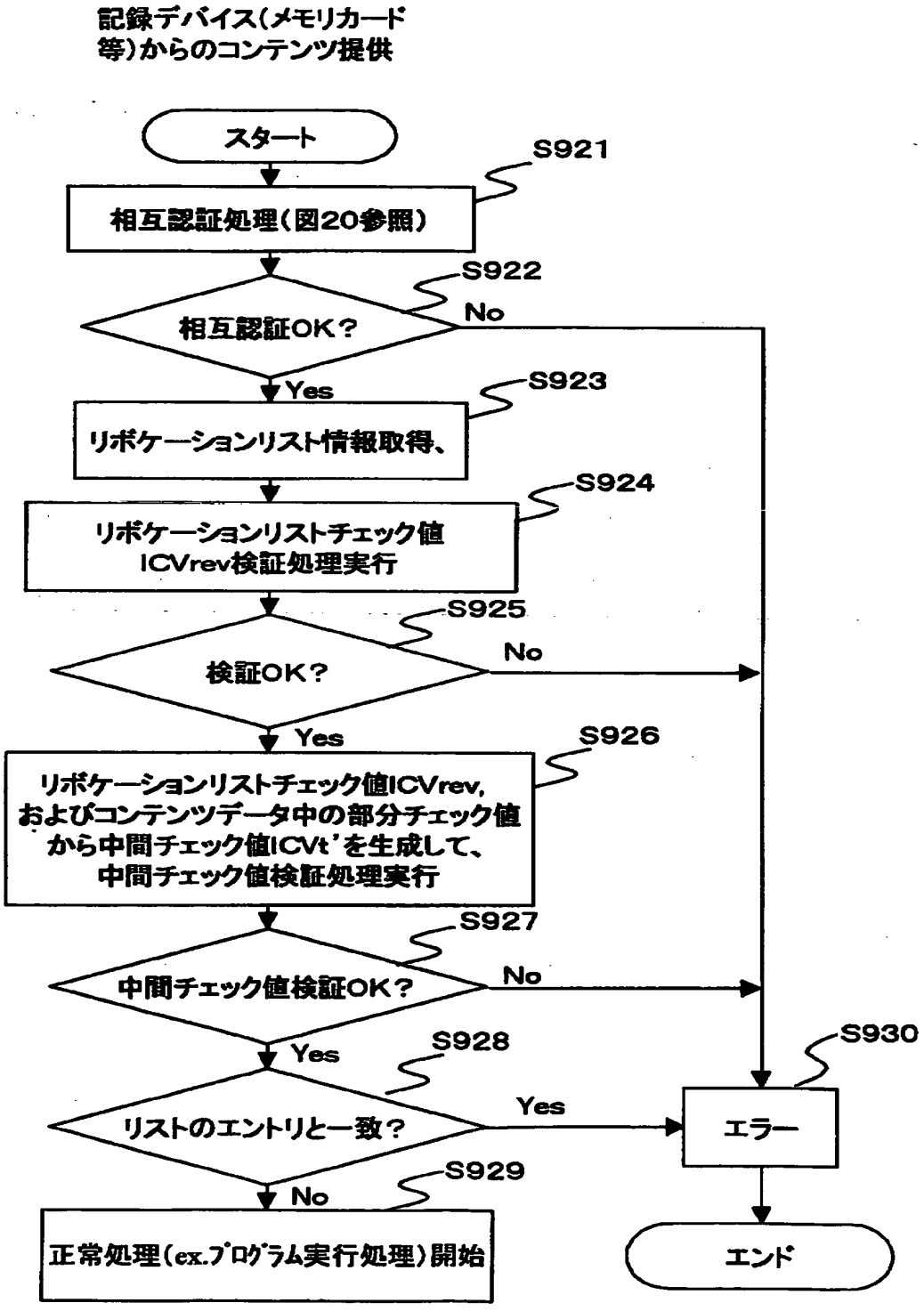
【図８６】


300
記録再生器
記録再生器識別子[IDdev]
配送鍵用マスター鍵[MKdis]
記録デバイス認証鍵用マスター鍵[MKake]
記録再生器署名鍵用マスター鍵[MKdev]
500
メディア
通信手段
600
400
記録デバイス
7701
識別情報
リボケーション(Revocation)リスト
リストチェック値ICVrev
コンテンツ
コンテンツ
コンテンツ
7702
7703

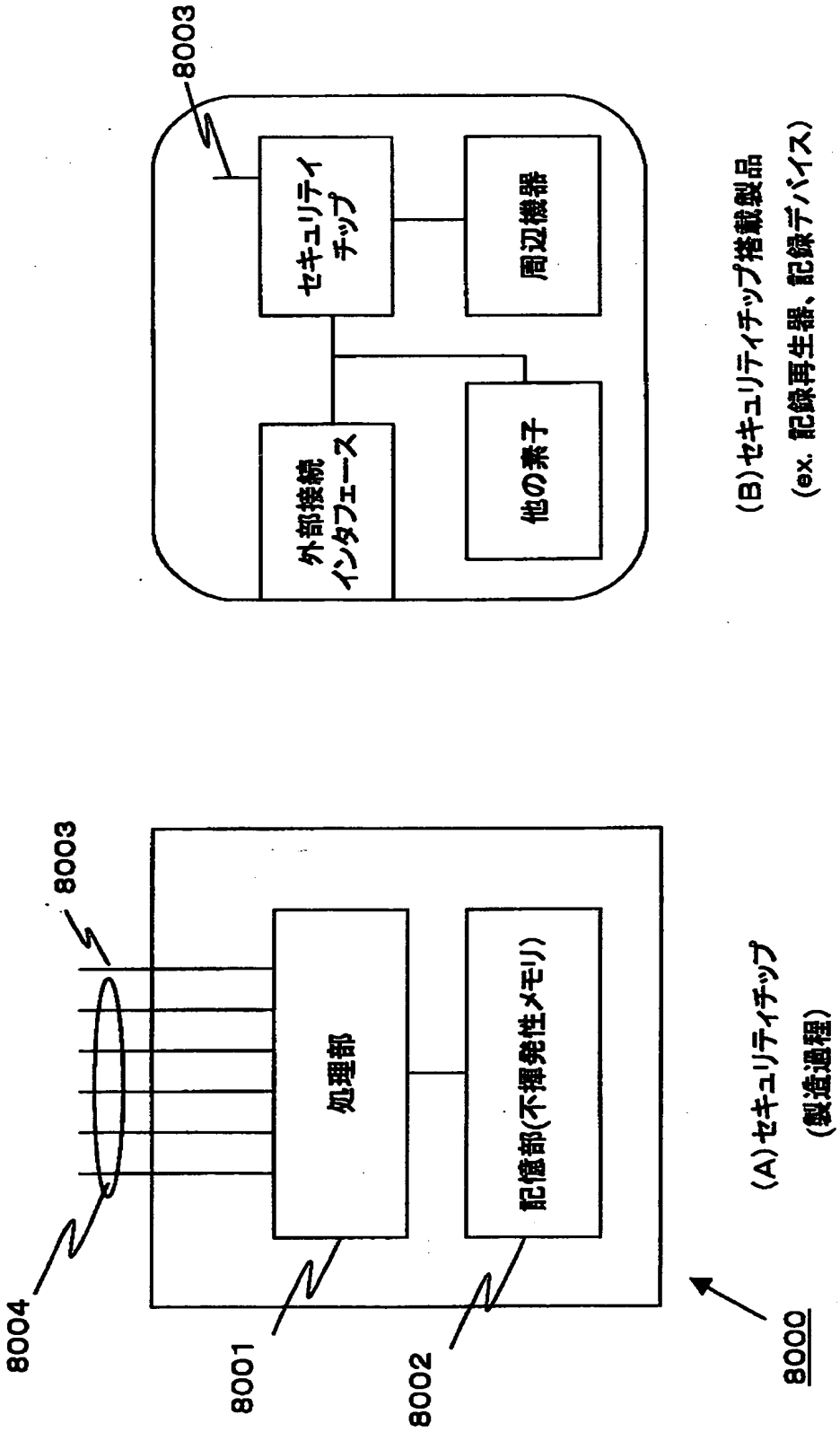
【図８７】


メディア(DVD, CD等)
からのコンテンツ提供
ネットワークからの
コンテンツ提供
スタート
スタート
S901
メディアに対する
コンテンツ提供要求
S911
配信サービス側と
通信セッション確立
S902
リポケーションリスト情報取得、
S903
リポケーションリストチェック値
ICVrev検証処理実行
S904
ICVrev検証OK？
No
Yes
S905
リポケーションリストチェック値ICVrev,
およびコンテンツデータ中の部分チェック値
から中間チェック値ICVt'を生成して、
中間チェック値検証処理実行
S906
中間チェック値検証OK？
No
Yes
S907
S909
リストのエントリと一致？
Yes
エラー
No
S908
正常処理(ex.プログラム実行処理)開始
エンド

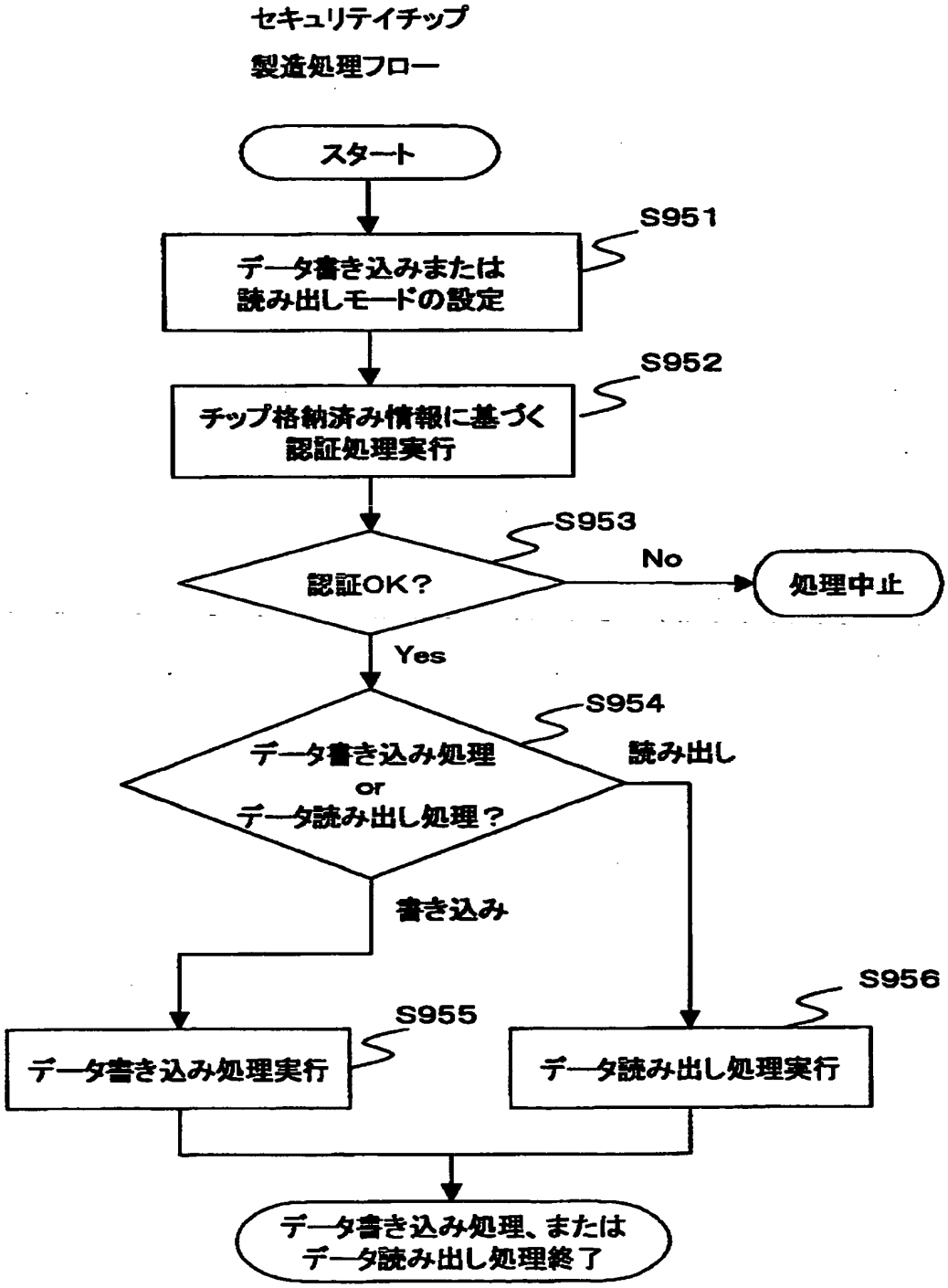
【図８８】


記録デバイス(メモリカード等)からのコンテンツ提供
スタート
S921
相互認証処理(図20参照)
S922
相互認証OK?
No
Yes
S923
リボケーションリスト情報取得、
S924
リボケーションリストチェック値ICVrev検証処理実行
S925
検証OK?
No
Yes
S926
リボケーションリストチェック値ICVrev,およびコンテンツデータ中の部分チェック値から中間チェック値ICVt'を生成して、中間チェック値検証処理実行
S927
中間チェック値検証OK?
No
Yes
S928
リストのエントリと一致?
Yes
S930
エラー
S929
No
正常処理(ex.ﾌﾟﾛｸﾞﾗﾑ実行処理)開始
エンド

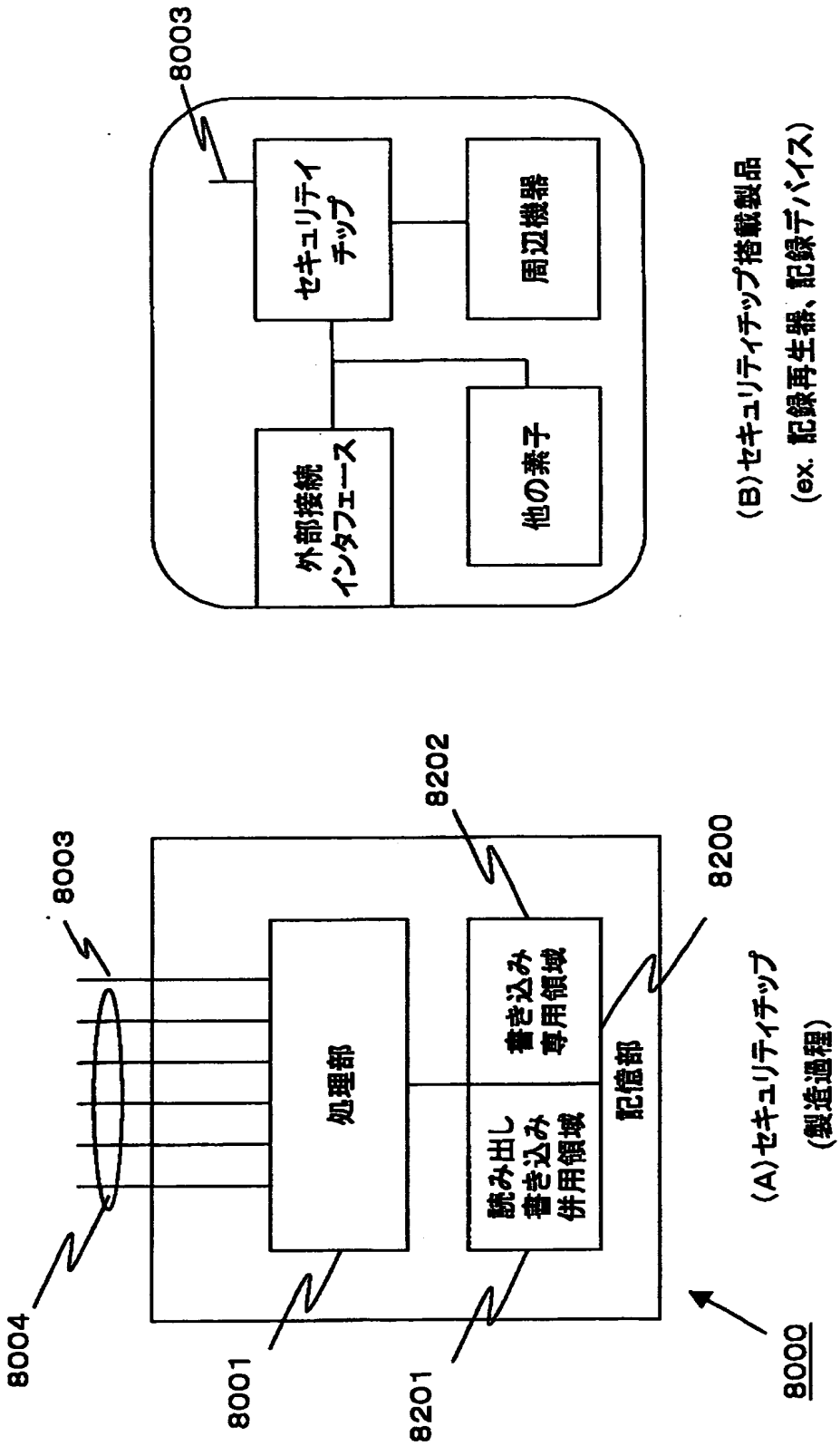
【図８９】


8003
セキュリティチップ
周辺機器
外部接続インタフェース
他の素子
(B)セキュリティチップ搭載製品
(ex. 記録再生器、記録デバイス)
8003
処理部
記憶部(不揮発性メモリ)
8004
8001
8002
8000
(A)セキュリティチップ
(製造過程)

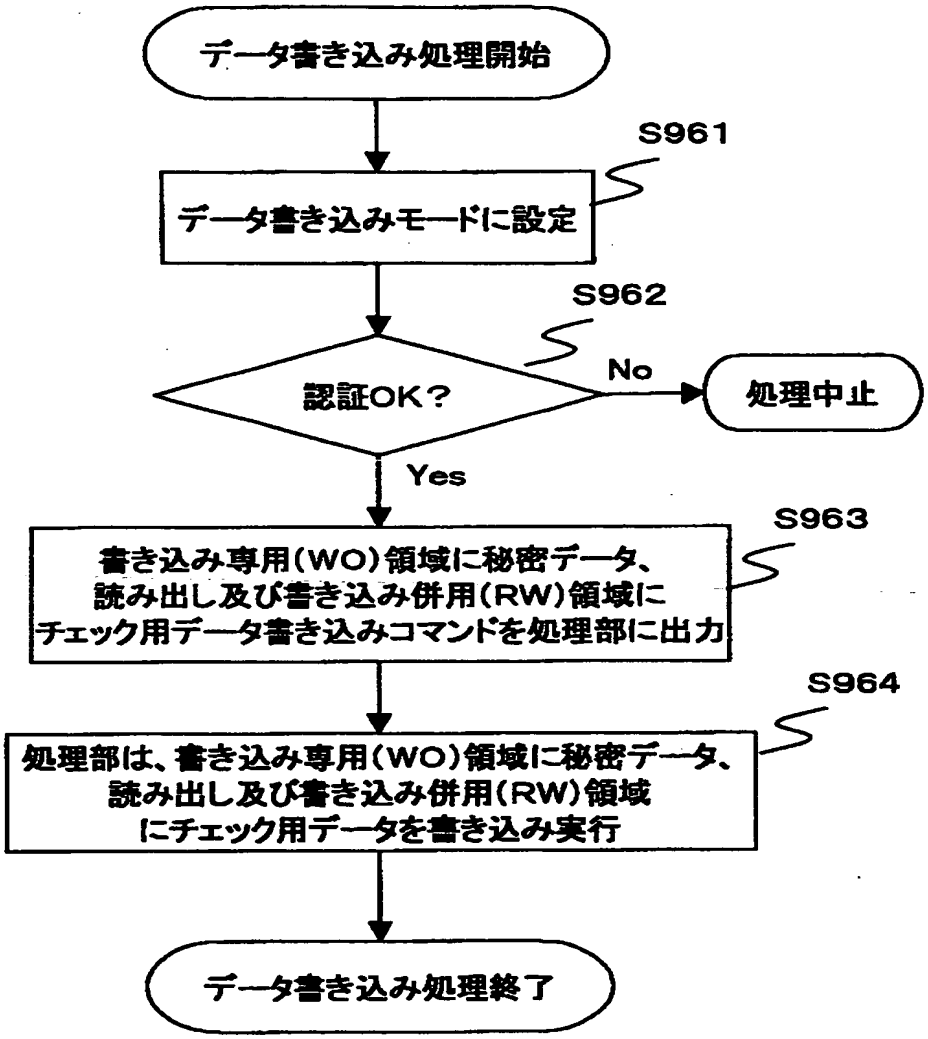
【図９０】


セキュリテイチップ
製造処理フロー
スタート
S951
データ書き込みまたは
読み出しモードの設定
S952
チップ格納済み情報に基づく
認証処理実行
S953
認証OK？
No
処理中止
Yes
S954
データ書き込み処理
or
データ読み出し処理？
読み出し
書き込み
S955
データ書き込み処理実行
S956
データ読み出し処理実行
データ書き込み処理、または
データ読み出し処理終了

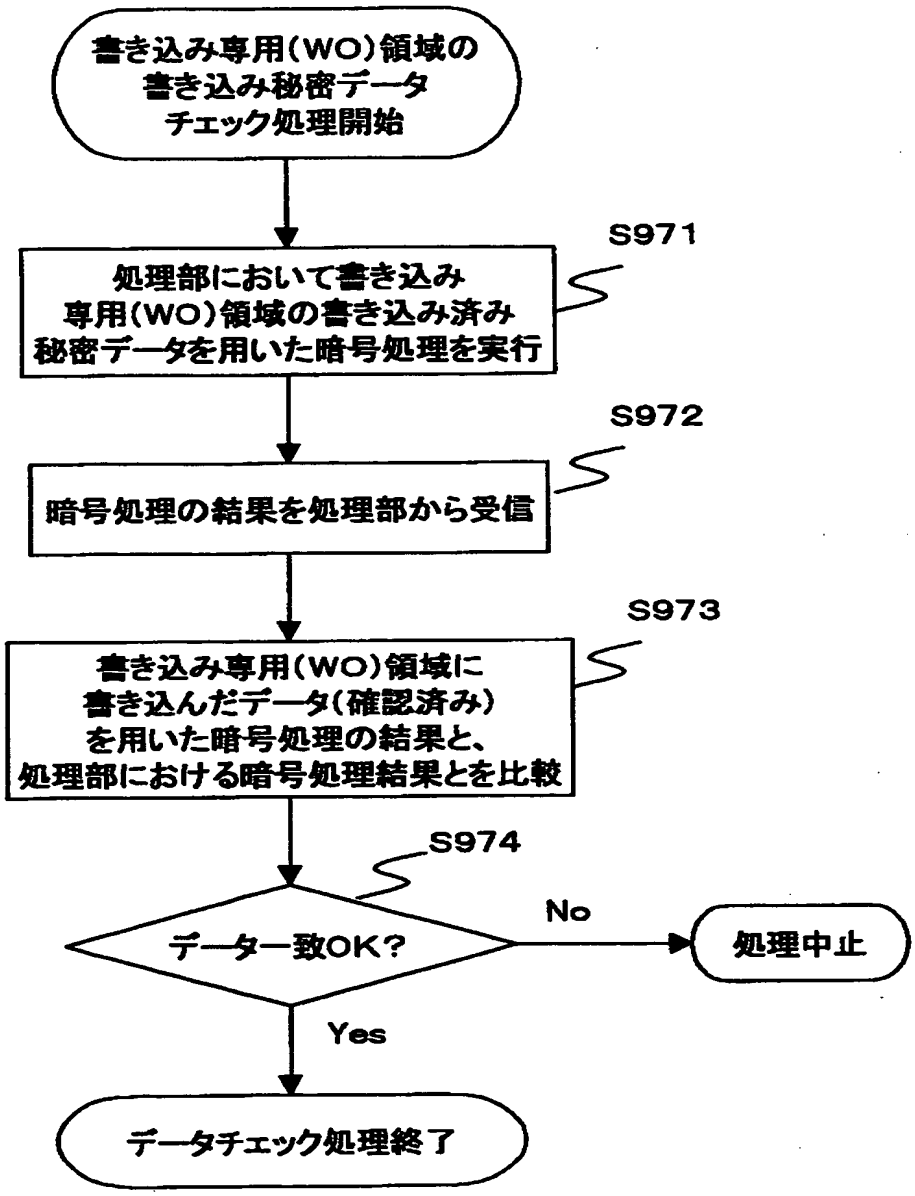
【図９１】


8003
セキュリティチップ
周辺機器
外部接続インタフェース
他の素子
(B)セキュリティチップ搭載製品
(ex. 記録再生器、記録デバイス)
8202
8200
8003
処理部
書き込み専用領域
読み出し書き込み併用領域
記憶部
(A)セキュリティチップ
(製造過程)
8004
8001
8201
8000

【図９２】


データ書き込み処理開始
S961
データ書き込みモードに設定
S962
認証OK？
No
処理中止
Yes
S963
書き込み専用(WO)領域に秘密データ、
読み出し及び書き込み併用(RW)領域に
チェック用データ書き込みコマンドを処理部に出力
S964
処理部は、書き込み専用(WO)領域に秘密データ、
読み出し及び書き込み併用(RW)領域
にチェック用データを書き込み実行
データ書き込み処理終了

【図９３】


書き込み専用(WO)領域の
書き込み秘密データ
チェック処理開始
S971
処理部において書き込み
専用(WO)領域の書き込み済み
秘密データを用いた暗号処理を実行
S972
暗号処理の結果を処理部から受信
S973
書き込み専用(WO)領域に
書き込んだデータ(確認済み)
を用いた暗号処理の結果と、
処理部における暗号処理結果とを比較
S974
データ一致OK?
No
処理中止
Yes
データチェック処理終了

【書類名】　　要約書

【要約】

【課題】　データ転送を実行する２つの装置間において、認証処理を前提としたコンテンツの利用を可能とするデータ処理装置を提供する。

【解決手段】　記録デバイスの暗号処理制御部が、認証処理、および格納データの暗号処理等に必要となるコマンドを、予め定めた設定シーケンスにしたがって実行する制御を実行する。制御部は、記録再生器から記録デバイスに送信されたコマンド番号を監視して、予め定めたシーケンスにしたがったコマンド番号のみを受け付けて実行する。コマンドシーケンスは、認証処理コマンドを暗号処理コマンドに先行して実行するように設定されているので、認証処理の済んだ記録再生器のみが記録デバイスに対するコンテンツの格納、または再生処理が実行でき、認証処理の済まない不正な機器によるコンテンツ利用が排除できる。

【選択図】　図２９

出 願 人 履 歴 情 報

識別番号　〔０００００２１８５〕

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社

出　願　人　履　歴　情　報

識別番号　　〔３９５０１５３１９〕

１．変更年月日　　１９９７年　３月３１日
［変更理由］　住所変更
住　所　東京都港区赤坂７－１－１
氏　名　株式会社ソニー・コンピュータエンタテインメント